

CompTIA SY0-401



CompTIA Security+ Certification

Version: 33.0

Topic 1, Network Security

QUESTION NO: 1

Sara, the security administrator, must configure the corporate firewall to allow all public IP addresses on the internal interface of the firewall to be translated to one public IP address on the external interface of the same firewall. Which of the following should Sara configure?

- A. PAT
- B. NAP
- C. DNAT
- D. NAC

Answer: A

Explanation:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

QUESTION NO: 2

Which of the following devices is MOST likely being used when processing the following?

1 PERMIT IP ANY ANY EQ 80

2 DENY IP ANY ANY

- A. Firewall
- B. NIPS
- C. Load balancer
- D. URL filter

Answer: A

Explanation:

Firewalls, routers, and even switches can use ACLs as a method of security management. An access control list has a deny ip any any implicitly at the end of any access control list. ACLs deny by default and allow by exception.

QUESTION NO: 3

The security administrator at ABC company received the following log information from an external party:

10:45:01 EST, SRC 10.4.3.7:3056, DST 8.4.2.1:80, ALERT, Directory traversal

10:45:02 EST, SRC 10.4.3.7:3057, DST 8.4.2.1:80, ALERT, Account brute force

10:45:03 EST, SRC 10.4.3.7:3058, DST 8.4.2.1:80, ALERT, Port scan

The external party is reporting attacks coming from abc-company.com. Which of the following is the reason the ABC company's security administrator is unable to determine the origin of the attack?

- A. A NIDS was used in place of a NIPS.
- B. The log is not in UTC.
- C. The external party uses a firewall.
- D. ABC company uses PAT.

Answer: D

Explanation:

PAT would ensure that computers on ABC's LAN translate to the same IP address, but with a different port number assignment. The log information shows the IP address, not the port number, making it impossible to pin point the exact source.

QUESTION NO: 4

Which of the following security devices can be replicated on a Linux based computer using IP tables to inspect and properly handle network based traffic?

- A. Sniffer
- B. Router

- C. Firewall
- D. Switch

Answer: C

Explanation:

Ip tables are a user-space application program that allows a system administrator to configure the tables provided by the Linux kernel firewall and the chains and rules it stores.

QUESTION NO: 5

Which of the following firewall types inspects Ethernet traffic at the MOST levels of the OSI model?

- A. Packet Filter Firewall
- B. Stateful Firewall
- C. Proxy Firewall
- D. Application Firewall

Answer: B

Explanation:

Stateful inspections occur at all levels of the network.

QUESTION NO: 6

The Chief Information Security Officer (CISO) has mandated that all IT systems with credit card data be segregated from the main corporate network to prevent unauthorized access and that access to the IT systems should be logged. Which of the following would BEST meet the CISO's requirements?

- A. Sniffers
- B. NIDS
- C. Firewalls
- D. Web proxies
- E. Layer 2 switches

Answer: C

Explanation:

The basic purpose of a firewall is to isolate one network from another.

QUESTION NO: 7

Which of the following network design elements allows for many internal devices to share one public IP address?

- A. DNAT
- B. PAT
- C. DNS
- D. DMZ

Answer: B

Explanation:

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

Most home networks use PAT. In such a scenario, the Internet Service Provider (ISP) assigns a single IP address to the home network's router. When Computer X logs on the Internet, the router assigns the client a port number, which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific packets to because each computer has a unique internal address.

QUESTION NO: 8

Which of the following is a best practice when securing a switch from physical access?

- A. Disable unnecessary accounts
- B. Print baseline configuration
- C. Enable access lists
- D. Disable unused ports

Answer: D

Explanation:

Disabling unused switch ports a simple method many network administrators use to help secure their network from unauthorized access.

All ports not in use should be disabled. Otherwise, they present an open door for an attacker to

enter.

QUESTION NO: 9

Which of the following devices would be MOST useful to ensure availability when there are a large number of requests to a certain website?

- A. Protocol analyzer
- B. Load balancer
- C. VPN concentrator
- D. Web security gateway

Answer: B

Explanation:

Load balancing refers to shifting a load from one device to another. A load balancer can be implemented as a software or hardware solution, and it is usually associated with a device—a router, a firewall, NAT appliance, and so on. In its most common implementation, a load balancer splits the traffic intended for a website into individual requests that are then rotated to redundant servers as they become available.

QUESTION NO: 10

Pete, the system administrator, wishes to monitor and limit users' access to external websites.

Which of the following would BEST address this?

- A. Block all traffic on port 80.
- B. Implement NIDS.
- C. Use server load balancers.
- D. Install a proxy server.

Answer: D

Explanation:

A proxy is a device that acts on behalf of other(s). In the interest of security, all internal user interaction with the Internet should be controlled through a proxy server. The proxy server should automatically block known malicious sites. The proxy server should cache often-accessed sites to improve performance.

QUESTION NO: 11

Mike, a network administrator, has been asked to passively monitor network traffic to the company's sales websites. Which of the following would be BEST suited for this task?

- A. HIDS
- B. Firewall
- C. NIPS
- D. Spam filter

Answer: C

Explanation:

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity.

QUESTION NO: 12

Which of the following should be deployed to prevent the transmission of malicious traffic between virtual machines hosted on a singular physical device on a network?

- A. HIPS on each virtual machine
- B. NIPS on the network
- C. NIDS on the network
- D. HIDS on each virtual machine

Answer: A

Explanation:

Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

QUESTION NO: 13

Pete, a security administrator, has observed repeated attempts to break into the network. Which of the following is designed to stop an intrusion on the network?

- A. NIPS
- B. HIDS
- C. HIPS
- D. NIDS

Answer: A

Explanation:

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

QUESTION NO: 14

An administrator is looking to implement a security device which will be able to not only detect network intrusions at the organization level, but help defend against them as well. Which of the following is being described here?

- A. NIDS
- B. NIPS
- C. HIPS
- D. HIDS

Answer: B

Explanation:

Network-based intrusion prevention system (NIPS) monitors the entire network for suspicious traffic by analyzing protocol activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

QUESTION NO: 15

In intrusion detection system vernacular, which account is responsible for setting the security policy for an organization?

- A. Supervisor
- B. Administrator
- C. Root
- D. Director

Answer: B

Explanation:

The administrator is the person responsible for setting the security policy for an organization and is responsible for making decisions about the deployment and configuration of the IDS.

QUESTION NO: 16

When performing the daily review of the system vulnerability scans of the network Joe, the administrator, noticed several security related vulnerabilities with an assigned vulnerability identification number. Joe researches the assigned vulnerability identification number from the vendor website. Joe proceeds with applying the recommended solution for identified vulnerability.

Which of the following is the type of vulnerability described?

- A. Network based
- B. IDS
- C. Signature based
- D. Host based

Answer: C

Explanation:

A signature-based monitoring or detection method relies on a database of signatures or patterns of known malicious or unwanted activity. The strength of a signature-based system is that it can quickly and accurately detect any event from its database of signatures.

QUESTION NO: 17

The network security engineer just deployed an IDS on the network, but the Chief Technical Officer (CTO) has concerns that the device is only able to detect known anomalies. Which of the following types of IDS has been deployed?

- A. Signature Based IDS
- B. Heuristic IDS
- C. Behavior Based IDS
- D. Anomaly Based IDS

Answer: A

Explanation:

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats.

QUESTION NO: 18

Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is

capable of alerting the team when unusual traffic is on the network. Which of the following types of technologies will BEST address this scenario?

- A. Application Firewall
- B. Anomaly Based IDS
- C. Proxy Firewall
- D. Signature IDS

Answer: B

Explanation:

Anomaly-based detection watches the ongoing activity in the environment and looks for abnormal occurrences. An anomaly-based monitoring or detection method relies on definitions of all valid forms of activity. This database of known valid activity allows the tool to detect any and all anomalies. Anomaly-based detection is commonly used for protocols. Because all the valid and legal forms of a protocol are known and can be defined, any variations from those known valid constructions are seen as anomalies.

QUESTION NO: 19

Matt, an administrator, notices a flood fragmented packet and retransmits from an email server.

After disabling the TCP offload setting on the NIC, Matt sees normal traffic with packets flowing in sequence again. Which of the following utilities was he MOST likely using to view this issue?

- A. Spam filter
- B. Protocol analyzer
- C. Web application firewall
- D. Load balancer

Answer: B

Explanation:

A protocol analyzer is a tool used to examine the contents of network traffic. Commonly known as a sniffer, a protocol analyzer can be a dedicated hardware device or software installed onto a typical host system. In either case, a protocol analyzer is first a packet capturing tool that can collect network traffic and store it in memory or onto a storage device. Once a packet is captured, it can be analyzed either with complex automated tools and scripts or manually.

QUESTION NO: 20

Which the following flags are used to establish a TCP connection? (Select TWO).

- A. PSH
- B. ACK
- C. SYN
- D. URG
- E. FIN

Answer: B,C

Explanation:

To establish a TCP connection, the three-way (or 3-step) handshake occurs:

SYN: The active open is performed by the client sending a SYN to the server. The client sets the segment's sequence number to a random value A.

SYN-ACK: In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number i.e. A+1, and the sequence number that the server chooses for the packet is another random number, B.

ACK: Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A+1, and the acknowledgement number is set to one more than the received sequence number i.e. B+1.

QUESTION NO: 21

Which of the following components of an all-in-one security appliance would MOST likely be configured in order to restrict access to peer-to-peer file sharing websites?

- A. Spam filter
- B. URL filter
- C. Content inspection
- D. Malware inspection

Answer: B

Explanation:

The question asks how to prevent access to peer-to-peer file sharing websites. You access a website by browsing to a URL using a Web browser or peer-to-peer file sharing client software. A URL filter is used to block URLs (websites) to prevent users accessing the website.

Incorrect Answer:

A: A spam filter is used for email. All inbound (and sometimes outbound) email is passed through the spam filter to detect spam emails. The spam emails are then discarded or tagged as potential spam according to the spam filter configuration. Spam filters do not prevent users accessing peer-to-peer file sharing websites.

C: Content inspection is the process of inspecting the content of a web page as it is downloaded.

The content can then be blocked if it doesn't comply with the company's web policy. Content-control software determines what content will be available or perhaps more often what content will be blocked. Content inspection does not prevent users accessing peer-to-peer file sharing websites (although it could block the content of the sites as it is downloaded).

D: Malware inspection is the process of scanning a computer system for malware. Malware inspection does not prevent users accessing peer-to-peer file sharing websites.

References:

<http://www.provision.ro/threat-management/web-application-security/url-filtering#pagei-1|pagep-1>
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 18, 19

QUESTION NO: 22

Pete, the system administrator, wants to restrict access to advertisements, games, and gambling web sites. Which of the following devices would BEST achieve this goal?

- A. Firewall
- B. Switch
- C. URL content filter
- D. Spam filter

Answer: C

Explanation:

URL filtering, also known as web filtering, is the act of blocking access to a site based on all or part of the URL used to request access. URL filtering can focus on all or part of a fully qualified domain name (FQDN), specific path names, specific filenames, specific file extensions, or entire specific URLs. Many URL-filtering tools can obtain updated master URL block lists from vendors as well as allow administrators to add or remove URLs from a custom list.

QUESTION NO: 23

The administrator receives a call from an employee named Joe. Joe says the Internet is down and he is receiving a blank page when typing to connect to a popular sports website. The administrator asks Joe to try visiting a popular search engine site, which Joe reports as successful. Joe then says that he can get to the sports site on this phone. Which of the following might the administrator need to configure?

- A. The access rules on the IDS

- B. The pop up blocker in the employee's browser
- C. The sensitivity level of the spam filter
- D. The default block page on the URL filter

Answer: D

Explanation:

A URL filter is used to block access to a site based on all or part of a URL. There are a number of URL-filtering tools that can acquire updated master URL block lists from vendors, as well as allow administrators to add or remove URLs from a custom list.

QUESTION NO: 24

Layer 7 devices used to prevent specific types of html tags are called:

- A. Firewalls
- B. Content filters
- C. Routers
- D. NIDS

Answer: B

Explanation:

A content filter is a type of software designed to restrict or control the content a reader is authorised to access, particularly when used to limit material delivered over the Internet via the Web, e-mail, or other means. Because the user and the OSI layer interact directly with the content filter, it operates at Layer 7 of the OSI model.

QUESTION NO: 25

Pete, an employee, attempts to visit a popular social networking site but is blocked. Instead, a page is displayed notifying him that this site cannot be visited. Which of the following is MOST likely blocking Pete's access to this site?

- A. Internet content filter
- B. Firewall
- C. Proxy server
- D. Protocol analyzer

Answer: A

Explanation:

Web filtering software is designed to restrict or control the content a reader is authorised to

access, especially when utilised to restrict material delivered over the Internet via the Web, e-mail, or other means.

QUESTION NO: 26

A review of the company's network traffic shows that most of the malware infections are caused by users visiting gambling and gaming websites. The security manager wants to implement a solution that will block these websites, scan all web traffic for signs of malware, and block the malware before it enters the company network. Which of the following is suited for this purpose?

- A. ACL
- B. IDS
- C. UTM
- D. Firewall

Answer: C

Explanation:

An all-in-one appliance, also known as Unified Threat Management (UTM) and Next Generation Firewall (NGFW), is one that provides a good foundation for security. A variety is available; those that you should be familiar with for the exam fall under the categories of providing URL filtering, content inspection, or malware inspection.

Malware inspection is the use of a malware scanner to detect unwanted software content in network traffic. If malware is detected, it can be blocked or logged and/or trigger an alert.

QUESTION NO: 27

Which of the following is BEST at blocking attacks and providing security at layer 7 of the OSI model?

- A. WAF
- B. NIDS
- C. Routers
- D. Switches

Answer: A

Explanation:

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site

scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

As the protocols used to access a web server (typically HTTP and HTTPS) run in layer 7 of the OSI model, then web application firewall (WAF) is the correct answer.

QUESTION NO: 28

Which of the following should the security administrator implement to limit web traffic based on country of origin? (Select THREE).

- A. Spam filter
- B. Load balancer
- C. Antivirus
- D. Proxies
- E. Firewall
- F. NIDS
- G. URL filtering

Answer: D,E,G

Explanation:

A proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers.

Firewalls manage traffic using a rule or a set of rules.

A URL is a reference to a resource that specifies the location of the resource. A URL filter is used to block access to a site based on all or part of a URL.

QUESTION NO: 29

A security engineer is reviewing log data and sees the output below:

POST: /payload.php HTTP/1.1

HOST: localhost

Accept: */*

Referrer: http://localhost/

HTTP/1.1 403 Forbidden

Connection: close

Log: Access denied with 403. Pattern matches form bypass Which of the following technologies was MOST likely being used to generate this log?

- A. Host-based Intrusion Detection System
- B. Web application firewall
- C. Network-based Intrusion Detection System
- D. Stateful Inspection Firewall
- E. URL Content Filter

Answer: B

Explanation:

A web application firewall is a device, server add-on, virtual service, or system filter that defines a strict set of communication rules for a website and all visitors. It's intended to be an application-specific firewall to prevent cross-site scripting, SQL injection, and other web application attacks.

QUESTION NO: 30

An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start?

- A. Review past security incidents and their resolution
- B. Rewrite the existing security policy
- C. Implement an intrusion prevention system
- D. Install honey pot systems

Answer: C

Explanation:

The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it

QUESTION NO: 31

A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability?

- A. Host-based firewall
- B. IDS
- C. IPS
- D. Honeypot

Answer: B

Explanation:

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

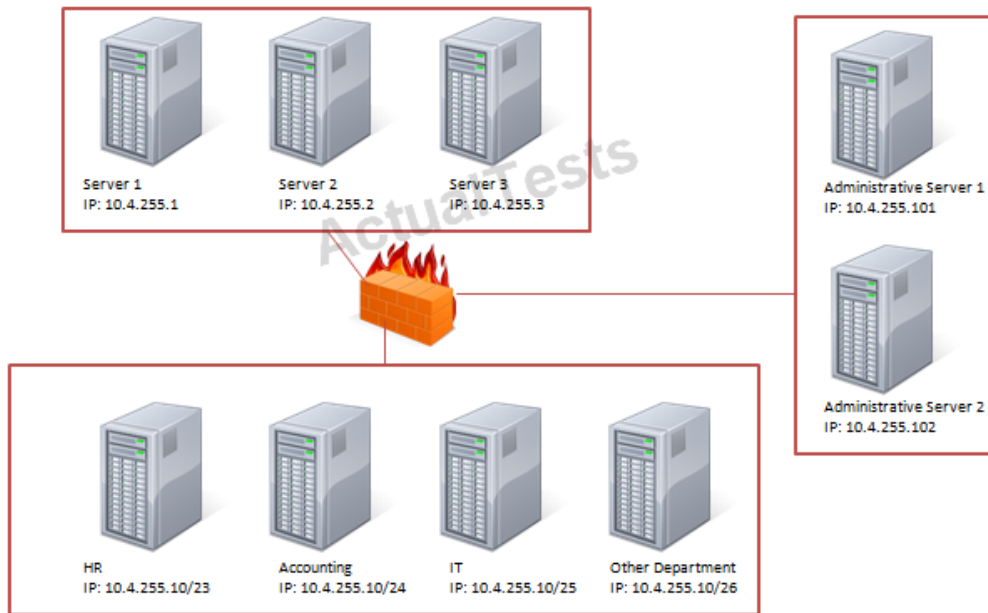
IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

QUESTION NO: 32 CORRECT TEXT

Configure the Firewall

Task: Configure the firewall (fill out the table) to allow these four rules:

1. Only allow the Accounting computer to have HTTPS access to the Administrative server.
2. Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
3. Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2



Source IP	Destination IP	Port Number	TCP/UDP	Allow/Deny

Answer: Use the following answer for this simulation task.

Source IP

Destination IP

Port number

TCP/UDP

Allow/Deny

10.4.255.10/24

10.4.255.101

443

TCP

Allow

10.4.255.10/23

10.4.255.2

22

TCP

Allow

10.4.255.10/25

10.4.255.101

Any

Any

Allow

10.4.255.10/25

10.4.255.102

Any

Any

Allow

Explanation:

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP. The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for acknowledging the correct reception of the data.

Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections – HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1)

Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)

Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:

10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

References:

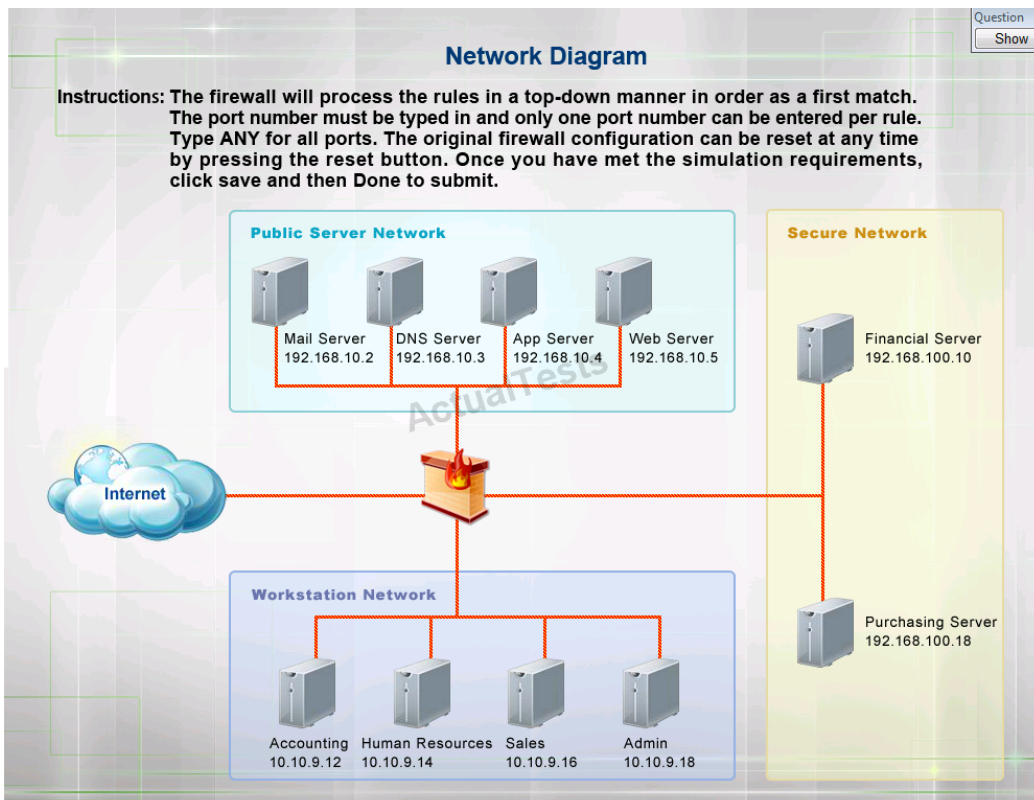
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 77, 83, 96, 157

QUESTION NO: 33 HOTSPOT

The security administrator has installed a new firewall which implements an implicit DENY policy by default. Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.

Instructions: The firewall will process the rules in a top-down manner in order as a first match. The port number must be typed in and only one port number can be entered per rule. Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.



Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1					
2					
3					
4					

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>
2	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>
3	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>
4	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>

Answer:

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>
2	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>
3	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>
4	<div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>10.10.9.12/32</div> <div>10.10.9.14/32</div> <div>10.10.9.18/32</div>	<div>Any</div> <div>192.168.10.2/32</div> <div>192.168.10.3/32</div> <div>192.168.10.4/32</div> <div>192.168.10.5/32</div> <div>192.168.100.10/32</div> <div>192.168.100.18/32</div>	<div>443</div> <div>22</div> <div>69</div>	<div>ANY</div> <div>TCP</div> <div>UDP</div>	<div>Permit</div> <div>Deny</div>

Explanation:

Firewall Rules					
Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	10.10.9.12/32	192.168.10.5/32	443	TCP	Permit
2	10.10.9.14/32	192.168.100.10/32	22	TCP	Permit
3	10.10.9.18/32	192.168.100.10/32	69	ANY	Permit
4	10.10.9.18/32	192.168.100.18/32	69	ANY	Permit

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.

Rule #1 allows the Accounting workstation to ONLY access the web server on the public network

over the default HTTPS port, which is TCP port 443.

Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22

Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION NO: 34

Which of the following firewall rules only denies DNS zone transfers?

- A. deny udp any any port 53
- B. deny ip any any
- C. deny tcp any any port 53
- D. deny all dns packets

Answer: C

Explanation:

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers.

QUESTION NO: 35

A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.

Which of the following would accomplish this task?

- A. Deny TCP port 68
- B. Deny TCP port 69
- C. Deny UDP port 68
- D. Deny UDP port 69

Answer: D

Explanation:

Trivial File Transfer Protocol (TFTP) is a simple file-exchange protocol that doesn't require

authentication. It operates on UDP port 69.

QUESTION NO: 36

Sara, a security technician, has received notice that a vendor coming in for a presentation will require access to a server outside of the network. Currently, users are only able to access remote sites through a VPN connection. How could Sara BEST accommodate the vendor?

- A. Allow incoming IPSec traffic into the vendor's IP address.
- B. Set up a VPN account for the vendor, allowing access to the remote site.
- C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.
- D. Write a firewall rule to allow the vendor to have access to the remote site.

Answer: D

Explanation:

Firewall rules are used to define what traffic is able pass between the firewall and the internal network. Firewall rules block the connection, allow the connection, or allow the connection only if it is secured. Firewall rules can be applied to inbound traffic or outbound traffic and any type of network.

QUESTION NO: 37

A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another?

- A. Implement a virtual firewall
- B. Install HIPS on each VM
- C. Virtual switches with VLANs
- D. Develop a patch management guide

Answer: C

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments.

QUESTION NO: 38

A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks.

Which of the following is MOST likely the reason for the sub-interfaces?

- A. The network uses the subnet of 255.255.255.128.
- B. The switch has several VLANs configured on it.
- C. The sub-interfaces are configured for VoIP traffic.
- D. The sub-interfaces each implement quality of service.

Answer: B

Explanation:

A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network.

QUESTION NO: 39

Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following actions should Joe recommend?

- A. Create a VLAN for the SCADA
- B. Enable PKI for the MainFrame
- C. Implement patch management
- D. Implement stronger WPA2 Wireless

Answer: A

Explanation:

VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN). Any network segment that doesn't need to communicate with another in order to accomplish a work task/function shouldn't be able to do so.

QUESTION NO: 40

The security administrator needs to manage traffic on a layer 3 device to support FTP from a new remote site. Which of the following would need to be implemented?

- A. Implicit deny
- B. VLAN management
- C. Port security
- D. Access control lists

Answer: D

Explanation:

In the OSI model, IP addressing and IP routing are performed at layer 3 (the network layer). In this question we need to configure routing. When configuring routing, you specify which IP range (in this case, the IP subnet of the remote site) is allowed to route traffic through the router to the FTP server.

Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

QUESTION NO: 41

Matt, the network engineer, has been tasked with separating network traffic between virtual machines on a single hypervisor. Which of the following would he implement to BEST address this requirement? (Select TWO).

- A. Virtual switch
- B. NAT
- C. System partitioning
- D. Access-list
- E. Disable spanning tree
- F. VLAN

Answer: A,F

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. A virtual switch is a software application that allows communication between virtual machines. A combination of the two would best satisfy the question.

QUESTION NO: 42

A database administrator contacts a security administrator to request firewall changes for a connection to a new internal application. The security administrator notices that the new application uses a port typically monopolized by a virus. The security administrator denies the request and suggests a new port or service be used to complete the application's task. Which of the following is the security administrator practicing in this example?

- A. Explicit deny
- B. Port security
- C. Access control lists
- D. Implicit deny

Answer: C

Explanation:

Traffic that comes into the router is compared to ACL entries based on the order that the entries occur in the router. New statements are added to the end of the list. The router continues to look until it has a match. If no matches are found when the router reaches the end of the list, the traffic is denied. For this reason, you should have the frequently hit entries at the top of the list. There is an implied deny for traffic that is not permitted.

QUESTION NO: 43

An administrator needs to connect a router in one building to a router in another using Ethernet. Each router is connected to a managed switch and the switches are connected to each other via a fiber line. Which of the following should be configured to prevent unauthorized devices from connecting to the network?

- A. Configure each port on the switches to use the same VLAN other than the default one
- B. Enable VTP on both switches and set to the same domain
- C. Configure only one of the routers to run DHCP services
- D. Implement port security on the switches

Answer: D

Explanation:

Port security in IT can mean several things:

The physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port.

The management of TCP and User Datagram Protocol (UDP) ports. If a service is active and assigned to a port, then that port is open. All the other 65,535 ports (of TCP or UDP) are closed if a service isn't actively using them.

Port knocking is a security system in which all ports on a system appear closed. However, if the

client sends packets to a specific set of ports in a certain order, a bit like a secret knock, then the desired service port becomes open and allows the client software to connect to the service.

QUESTION NO: 44

At an organization, unauthorized users have been accessing network resources via unused network wall jacks. Which of the following would be used to stop unauthorized access?

- A. Configure an access list.
- B. Configure spanning tree protocol.
- C. Configure port security.
- D. Configure loop protection.

Answer: C

Explanation:

Port security in IT can mean several things. It can mean the physical control of all connection points, such as RJ-45 wall jacks or device ports, so that no unauthorized users or unauthorized devices can attempt to connect into an open port. This can be accomplished by locking down the wiring closet and server vaults and then disconnecting the workstation run from the patch panel (or punch-down block) that leads to a room's wall jack. Any unneeded or unused wall jacks can (and should) be physically disabled in this manner. Another option is to use a smart patch panel that can monitor the MAC address of any device connected to each and every wall port across a building and detect not just when a new device is connected to an empty port, but also when a valid device is disconnected or replaced by an invalid device.

QUESTION NO: 45

On Monday, all company employees report being unable to connect to the corporate wireless network, which uses 802.1x with PEAP. A technician verifies that no configuration changes were made to the wireless network and its supporting infrastructure, and that there are no outages.

Which of the following is the MOST likely cause for this issue?

- A. Too many incorrect authentication attempts have caused users to be temporarily disabled.
- B. The DNS server is overwhelmed with connections and is unable to respond to queries.
- C. The company IDS detected a wireless attack and disabled the wireless network.
- D. The Remote Authentication Dial-In User Service server certificate has expired.

Answer: D

Explanation:

The question states that the network uses 802.1x with PEAP. The 802.1x authentication server is typically an EAP-compliant Remote Access Dial-In User Service (RADIUS). A RADIUS server will be configured with a digital certificate. When a digital certificate is created, an expiration period is configured by the Certificate Authority (CA). The expiration period is commonly one or two years. The question states that no configuration changes have been made so it's likely that the certificate has expired.

QUESTION NO: 46

A company determines a need for additional protection from rogue devices plugging into physical ports around the building.

Which of the following provides the highest degree of protection from unauthorized wired network access?

- A. Intrusion Prevention Systems
- B. MAC filtering
- C. Flood guards
- D. 802.1x

Answer: D

Explanation:

IEEE 802.1x is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to wireless devices connecting to a LAN or WLAN.

QUESTION NO: 47

While configuring a new access layer switch, the administrator, Joe, was advised that he needed to make sure that only devices authorized to access the network would be permitted to login and utilize resources. Which of the following should the administrator implement to ensure this happens?

- A. Log Analysis
- B. VLAN Management
- C. Network separation
- D. 802.1x

Answer: D

Explanation:

802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

QUESTION NO: 48

A network administrator wants to block both DNS requests and zone transfers coming from outside IP addresses. The company uses a firewall which implements an implicit allow and is currently configured with the following ACL applied to its external interface.

PERMIT TCP ANY ANY 80

PERMIT TCP ANY ANY 443

Which of the following rules would accomplish this task? (Select TWO).

A. Change the firewall default settings so that it implements an implicit deny

B. Apply the current ACL to all interfaces of the firewall

C. Remove the current ACL

D. Add the following ACL at the top of the current ACL

DENY TCP ANY ANY 53

E. Add the following ACL at the bottom of the current ACL

DENY ICMP ANY ANY 53

F. Add the following ACL at the bottom of the current ACL

DENY IP ANY ANY 53

Answer: A,F

Explanation:

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Implicit deny is the default response when an explicit allow or deny isn't present.

DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. These are zone file exchanges between DNS servers, special manual queries, or used when a response exceeds 512 bytes. UDP port 53 is used for most typical DNS queries.

QUESTION NO: 49

Users are unable to connect to the web server at IP 192.168.0.20. Which of the following can be inferred of a firewall that is configured ONLY with the following ACL?

PERMIT TCP ANY HOST 192.168.0.10 EQ 80

PERMIT TCP ANY HOST 192.168.0.10 EQ 443

- A. It implements stateful packet filtering.
- B. It implements bottom-up processing.
- C. It failed closed.
- D. It implements an implicit deny.

Answer: D

Explanation:

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default. Implicit deny is the default response when an explicit allow or deny isn't present.

QUESTION NO: 50

The Human Resources department has a parent shared folder setup on the server. There are two groups that have access, one called managers and one called staff. There are many sub folders under the parent shared folder, one is called payroll. The parent folder access control list propagates all subfolders and all subfolders inherit the parent permission. Which of the following is the quickest way to prevent the staff group from gaining access to the payroll folder?

- A. Remove the staff group from the payroll folder
- B. Implicit deny on the payroll folder for the staff group
- C. Implicit deny on the payroll folder for the managers group
- D. Remove inheritance from the payroll folder

Answer: B

Explanation: Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.

QUESTION NO: 51

A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements?

- A. NAT and DMZ
- B. VPN and IPSec
- C. Switches and a firewall
- D. 802.1x and VLANs

Answer: D

Explanation:

802.1x is a port-based authentication mechanism. It's based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it's often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System's Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. But as the switch administrator changes the VLAN assignment on a port-by-port basis, various ports can be grouped together and be distinct from other VLAN port designations. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION NO: 52

Matt, the IT Manager, wants to create a new network available to virtual servers on the same hypervisor, and does not want this network to be routable to the firewall. How could this BEST be accomplished?

- A. Create a VLAN without a default gateway.
- B. Remove the network from the routing table.
- C. Create a virtual switch.
- D. Commission a stand-alone switch.

Answer: C

Explanation:

A Hyper-V Virtual Switch implements policy enforcement for security, isolation, and service levels.

QUESTION NO: 53

A Chief Information Security Officer (CISO) is tasked with outsourcing the analysis of security logs. These will need to still be reviewed on a regular basis to ensure the security of the company has not been breached. Which of the following cloud service options would support this requirement?

- A. SaaS
- B. MaaS
- C. IaaS
- D. PaaS

Answer: B

Explanation:

Monitoring-as-a-service (MaaS) is a cloud delivery model that falls under anything as a service (XaaS). MaaS allows for the deployment of monitoring functionalities for several other services and applications within the cloud.

QUESTION NO: 54

Joe, a security administrator, believes that a network breach has occurred in the datacenter as a result of a misconfigured router access list, allowing outside access to an SSH server. Which of the following should Joe search for in the log files?

- A. Failed authentication attempts
- B. Network ping sweeps
- C. Host port scans
- D. Connections to port 22

Answer: D

Explanation:

Log analysis is the art and science of reviewing audit trails, log files, or other forms of computer-generated records for evidence of policy violations, malicious events, downtimes, bottlenecks, or other issues of concern.

SSH uses TCP port 22. All protocols encrypted by SSH also use TCP port 22, such as SFTP, SHTTP, SCP, SExec, and slogin.

QUESTION NO: 55

An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to combine the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

- A. Unified Threat Management
- B. Virtual Private Network
- C. Single sign on
- D. Role-based management

Answer: A

Explanation:

When you combine a firewall with other abilities (intrusion prevention, antivirus, content filtering, etc.), what used to be called an all-in-one appliance is now known as a unified threat management (UTM) system. The advantages of combining everything into one include a reduced learning curve (you only have one product to learn), a single vendor to deal with, and—typically—reduced complexity.

QUESTION NO: 56

An organization does not have adequate resources to administer its large infrastructure. A security administrator wishes to integrate the security controls of some of the network devices in the organization. Which of the following methods would BEST accomplish this goal?

- A. Unified Threat Management
- B. Virtual Private Network
- C. Single sign on
- D. Role-based management

Answer: A

Explanation:

Unified Threat Management (UTM) is, basically, the combination of a firewall with other abilities. These abilities include intrusion prevention, antivirus, content filtering, etc. Advantages of combining everything into one:

You only have one product to learn.

You only have to deal with a single vendor.

IT provides reduced complexity.

QUESTION NO: 57

A security administrator is segregating all web-facing server traffic from the internal network and restricting it to a single interface on a firewall. Which of the following BEST describes this new network?

- A. VLAN
- B. Subnet
- C. VPN
- D. DMZ

Answer: D

Explanation:

A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network. The name is derived from the term "demilitarized zone", an area between nation states in which military operation is not permitted.

QUESTION NO: 58

Which of the following devices would MOST likely have a DMZ interface?

- A. Firewall
- B. Switch
- C. Load balancer
- D. Proxy

Answer: A

Explanation: The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

QUESTION NO: 59

A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

- A. DMZ

- B. Cloud computing
- C. VLAN
- D. Virtualization

Answer: A

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

QUESTION NO: 60

Which of the following network architecture concepts is used to securely isolate at the boundary between networks?

- A. VLAN
- B. Subnetting
- C. DMZ
- D. NAT

Answer: C

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

QUESTION NO: 61

When designing a new network infrastructure, a security administrator requests that the intranet web server be placed in an isolated area of the network for security purposes. Which of the following design elements would be implemented to comply with the security administrator's request?

- A. DMZ
- B. Cloud services
- C. Virtualization
- D. Sandboxing

Answer: A

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

QUESTION NO: 62

Which of the following BEST describes a demilitarized zone?

- A. A buffer zone between protected and unprotected networks.
- B. A network where all servers exist and are monitored.
- C. A sterile, isolated network segment with access lists.
- D. A private network that is protected by a firewall and a VLAN.

Answer: A

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted LAN. Often a DMZ is deployed through the use of a multihomed firewall.

QUESTION NO: 63

Which of the following would allow the organization to divide a Class C IP address range into several ranges?

- A. DMZ
- B. Virtual LANs
- C. NAT
- D. Subnetting

Answer: D

Explanation:

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

QUESTION NO: 64

Which of the following IP addresses would be hosts on the same subnet given the subnet mask 255.255.255.224? (Select TWO).

- A. 10.4.4.125
- B. 10.4.4.158
- C. 10.4.4.165
- D. 10.4.4.189
- E. 10.4.4.199

Answer: C,D

Explanation:

With the given subnet mask, a maximum number of 30 hosts between IP addresses 10.4.4.161 and 10.4.4.190 are allowed. Therefore, option C and D would be hosts on the same subnet, and the other options would not.

References:

<http://www.subnetonline.com/pages/subnet-calculators/ip-subnet-calculator.php>

QUESTION NO: 65

Which of the following would the security engineer set as the subnet mask for the servers below to utilize host addresses on separate broadcast domains?

Server 1: 192.168.100.6

Server 2: 192.168.100.9

Server 3: 192.169.100.20

- A. /24
- B. /27
- C. /28
- D. /29
- E. /30

Answer: D

Explanation:

Using this option will result in all three servers using host addresses on different broadcast domains.

QUESTION NO: 66

Which of the following is BEST used to break a group of IP addresses into smaller network segments or blocks?

- A. NAT
- B. Virtualization
- C. NAC
- D. Subnetting

Answer: D

Explanation:

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

QUESTION NO: 67

A small company can only afford to buy an all-in-one wireless router/switch. The company has 3 wireless BYOD users and 2 web servers without wireless access. Which of the following should the company configure to protect the servers from the user devices? (Select TWO).

- A. Deny incoming connections to the outside router interface.
- B. Change the default HTTP port
- C. Implement EAP-TLS to establish mutual authentication
- D. Disable the physical switch ports
- E. Create a server VLAN
- F. Create an ACL to access the server

Answer: E,F

Explanation:

We can protect the servers from the user devices by separating them into separate VLANs (virtual local area networks).

The network device in the question is a router/switch. We can use the router to allow access from devices in one VLAN to the servers in the other VLAN. We can configure an ACL (Access Control List) on the router to determine who is able to access the server.

In computer networking, a single layer-2 network may be partitioned to create multiple distinct broadcast domains, which are mutually isolated so that packets can only pass between them via one or more routers; such a domain is referred to as a virtual local area network, virtual LAN or VLAN.

This is usually achieved on switch or router devices. Simpler devices only support partitioning on a port level (if at all), so sharing VLANs across devices requires running dedicated cabling for each

VLAN. More sophisticated devices can mark packets through tagging, so that a single interconnect (trunk) may be used to transport data for multiple VLANs.

Grouping hosts with a common set of requirements regardless of their physical location by VLAN can greatly simplify network design. A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if they are not on the same network switch. The network described in this question is a DMZ, not a VLAN.

QUESTION NO: 68

A network engineer is setting up a network for a company. There is a BYOD policy for the employees so that they can connect their laptops and mobile devices.

Which of the following technologies should be employed to separate the administrative network from the network in which all of the employees' devices are connected?

- A. VPN
- B. VLAN
- C. WPA2
- D. MAC filtering

Answer: B

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION NO: 69

Pete, a network administrator, is capturing packets on the network and notices that a large amount of the traffic on the LAN is SIP and RTP protocols. Which of the following should he do to segment that traffic from the other traffic?

- A. Connect the WAP to a different switch.
- B. Create a voice VLAN.
- C. Create a DMZ.
- D. Set the switch ports to 802.1q mode.

Answer: B

Explanation:

It is a common and recommended practice to separate voice and data traffic by using VLANs. Separating voice and data traffic using VLANs provides a solid security boundary, preventing data applications from reaching the voice traffic. It also gives you a simpler method to deploy QoS, prioritizing the voice traffic over the data.

QUESTION NO: 70

An administrator connects VoIP phones to the same switch as the network PCs and printers. Which of the following would provide the BEST logical separation of these three device types while still allowing traffic between them via ACL?

- A. Create three VLANs on the switch connected to a router
- B. Define three subnets, configure each device to use their own dedicated IP address range, and then connect the network to a router
- C. Install a firewall and connect it to the switch
- D. Install a firewall and connect it to a dedicated switch for each device type

Answer: A

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION NO: 71

An administrator needs to segment internal traffic between layer 2 devices within the LAN. Which of the following types of network design elements would MOST likely be used?

- A. Routing
- B. DMZ
- C. VLAN
- D. NAT

Answer: C

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the

same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION NO: 72

Pete, a security administrator, is informed that people from the HR department should not have access to the accounting department's server, and the accounting department should not have access to the HR department's server. The network is separated by switches. Which of the following is designed to keep the HR department users from accessing the accounting department's server and vice-versa?

- A. ACLs
- B. VLANs
- C. DMZs
- D. NATS

Answer: B

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION NO: 73

According to company policy an administrator must logically keep the Human Resources department separated from the Accounting department. Which of the following would be the simplest way to accomplish this?

- A. NIDS
- B. DMZ
- C. NAT
- D. VLAN

Answer: D

Explanation: A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches.

QUESTION NO: 74

Review the following diagram depicting communication between PC1 and PC2 on each side of a router. Analyze the network traffic logs which show communication between the two computers as captured by the computer with IP 10.2.2.10.

DIAGRAM

PC1 PC2

[192.168.1.30]-----[INSIDE 192.168.1.1 router OUTSIDE 10.2.2.1]-----[10.2.2.10] LOGS

10:30:22, SRC 10.2.2.1:3030, DST 10.2.2.10:80, SYN

10:30:23, SRC 10.2.2.10:80, DST 10.2.2.1:3030, SYN/ACK

10:30:24, SRC 10.2.2.1:3030, DST 10.2.2.10:80, ACK

Given the above information, which of the following can be inferred about the above environment?

- A. 192.168.1.30 is a web server.
- B. The web server listens on a non-standard port.
- C. The router filters port 80 traffic.
- D. The router implements NAT.

Answer: D

Explanation:

Network address translation (NAT) allows you to share a connection to the public Internet via a single interface with a single public IP address. NAT maps the private addresses to the public address. In a typical configuration, a local network uses one of the designated "private" IP address subnets. A router on that network has a private address (192.168.1.1) in that address space, and is also connected to the Internet with a "public" address (10.2.2.1) assigned by an Internet service provider.

QUESTION NO: 75

An administrator wishes to hide the network addresses of an internal network when connecting to the Internet. The MOST effective way to mask the network address of the users would be by passing the traffic through a:

- A. stateful firewall
- B. packet-filtering firewall

- C. NIPS
- D. NAT

Answer: D

Explanation:

NAT serves as a basic firewall by only allowing incoming traffic that is in response to an internal system's request.

QUESTION NO: 76

A security analyst is reviewing firewall logs while investigating a compromised web server. The following ports appear in the log:

22, 25, 445, 1433, 3128, 3389, 6667

Which of the following protocols was used to access the server remotely?

- A. LDAP
- B. HTTP
- C. RDP
- D. HTTPS

Answer: C

Explanation:

RDP uses TCP port 3389.

QUESTION NO: 77

Which of the following is a programming interface that allows a remote computer to run programs on a local machine?

- A. RPC
- B. RSH
- C. SSH
- D. SSL

Answer: A

Explanation:

Remote Procedure Call (RPC) is a programming interface that allows a remote computer to run

programs on a local machine.

QUESTION NO: 78

Which of the following would Pete, a security administrator, MOST likely implement in order to allow employees to have secure remote access to certain internal network services such as file servers?

- A. Packet filtering firewall
- B. VPN gateway
- C. Switch
- D. Router

Answer: B

Explanation:

VPNs are usually employed to allow remote access users to connect to and access the network, and offer connectivity between two or more private networks or LANs. A VPN gateway (VPN router) is a connection point that connects two LANs via a nonsecure network such as the Internet.

QUESTION NO: 79

Which of the following should be performed to increase the availability of IP telephony by prioritizing traffic?

- A. Subnetting
- B. NAT
- C. Quality of service
- D. NAC

Answer: C

Explanation:

Quality of Service (QoS) facilitates the deployment of media-rich applications, such as video conferencing and Internet Protocol (IP) telephony, without adversely affecting network throughput.

QUESTION NO: 80

An auditor is given access to a conference room to conduct an analysis. When they connect their laptop's Ethernet cable into the wall jack, they are not able to get a connection to the Internet but

have a link light. Which of the following is MOST likely causing this issue?

- A. Ethernet cable is damaged
- B. The host firewall is set to disallow outbound connections
- C. Network Access Control
- D. The switch port is administratively shutdown

Answer: C

Explanation:

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

QUESTION NO: 81

A computer is put into a restricted VLAN until the computer's virus definitions are up-to-date.

Which of the following BEST describes this system type?

- A. NAT
- B. NIPS
- C. NAC
- D. DMZ

Answer: C

Explanation:

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies. The goals of NAC are to prevent/reduce zero-day attacks, enforce security policy throughout the network, and use identities to perform access control.

QUESTION NO: 82

Which of the following is required to allow multiple servers to exist on one physical server?

- A. Software as a Service (SaaS)
- B. Platform as a Service (PaaS)
- C. Virtualization
- D. Infrastructure as a Service (IaaS)

Answer: C

Explanation:

Virtualization allows a single set of hardware to host multiple virtual machines.

QUESTION NO: 83

A corporation is looking to expand their data center but has run out of physical space in which to store hardware. Which of the following would offer the ability to expand while keeping their current data center operated by internal staff?

- A. Virtualization
- B. Subnetting
- C. IaaS
- D. SaaS

Answer: A

Explanation:

Virtualization allows a single set of hardware to host multiple virtual machines.

QUESTION NO: 84

The server administrator has noted that most servers have a lot of free disk space and low memory utilization. Which of the following statements will be correct if the server administrator migrates to a virtual server environment?

- A. The administrator will need to deploy load balancing and clustering.
- B. The administrator may spend more on licensing but less on hardware and equipment.
- C. The administrator will not be able to add a test virtual environment in the data center.
- D. Servers will encounter latency and lowered throughput issues.

Answer: B

Explanation:

Migrating to a virtual server environment reduces cost by eliminating the need to purchase, manage, maintain and power physical machines. The fewer physical machines you have, the less money it costs.

QUESTION NO: 85

Due to limited resources, a company must reduce their hardware budget while still maintaining availability. Which of the following would MOST likely help them achieve their objectives?

- A. Virtualization
- B. Remote access
- C. Network access control
- D. Blade servers

Answer: A

Explanation:

Because Virtualization allows a single set of hardware to host multiple virtual machines, it requires less hardware to maintain the current scenario.

QUESTION NO: 86

Pete, a security engineer, is trying to inventory all servers in a rack. The engineer launches RDP sessions to five different PCs and notices that the hardware properties are similar. Additionally, the MAC addresses of all five servers appear on the same switch port. Which of the following is MOST likely the cause?

- A. The system is running 802.1x.
- B. The system is using NAC.
- C. The system is in active-standby mode.
- D. The system is virtualized.

Answer: D

Explanation:

Virtualization allows a single set of hardware to host multiple virtual machines.

QUESTION NO: 87

Which of the following offers the LEAST amount of protection against data theft by USB drives?

- A. DLP
- B. Database encryption
- C. TPM
- D. Cloud computing

Answer: D

Explanation:

Cloud computing refers to performing data processing and storage elsewhere, over a network connection, rather than locally. Because users have access to the data, it can easily be copied to a USB device.

QUESTION NO: 88

A company's business model was changed to provide more web presence and now its ERM software is no longer able to support the security needs of the company. The current data center will continue to provide network and security services. Which of the following network elements would be used to support the new business model?

- A. Software as a Service
- B. DMZ
- C. Remote access support
- D. Infrastructure as a Service

Answer: A

Explanation:

Software as a Service (SaaS) allows for on-demand online access to specific software applications or suites without having to install it locally. This will allow the data center to continue providing network and security services.

QUESTION NO: 89

The Chief Information Officer (CIO) has mandated web based Customer Relationship Management (CRM) business functions be moved offshore to reduce cost, reduce IT overheads, and improve availability. The Chief Risk Officer (CRO) has agreed with the CIO's direction but has mandated that key authentication systems be run within the organization's network. Which of the following would BEST meet the CIO and CRO's requirements?

- A. Software as a Service
- B. Infrastructure as a Service
- C. Platform as a Service
- D. Hosted virtualization service

Answer: A

Explanation:

Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

QUESTION NO: 90

An IT director is looking to reduce the footprint of their company's server environment. They have decided to move several internally developed software applications to an alternate environment, supported by an external company. Which of the following BEST describes this arrangement?

- A. Infrastructure as a Service
- B. Storage as a Service
- C. Platform as a Service
- D. Software as a Service

Answer: A

Explanation:

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

QUESTION NO: 91

Which of the following offerings typically allows the customer to apply operating system patches?

- A. Software as a service
- B. Public Clouds
- C. Cloud Based Storage
- D. Infrastructure as a service

Answer: D

Explanation:

Cloud users install operating-system images and their application software on the cloud infrastructure to deploy their applications. In this model, the cloud user patches and maintains the operating systems and the application software.

QUESTION NO: 92

Which of the following technologies can store multi-tenant data with different security requirements?

- A. Data loss prevention
- B. Trusted platform module
- C. Hard drive encryption
- D. Cloud computing

Answer: D

Explanation:

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This “multitenant” nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security.

QUESTION NO: 93

Multi-tenancy is a concept found in which of the following?

- A. Full disk encryption
- B. Removable media
- C. Cloud computing
- D. Data loss prevention

Answer: C

Explanation:

One of the ways cloud computing is able to obtain cost efficiencies is by putting data from various clients on the same machines. This “multitenant” nature means that workloads from different clients can be on the same system, and a flaw in implementation could compromise security.

QUESTION NO: 94

Which of the following devices is BEST suited to protect an HTTP-based application that is susceptible to injection attacks?

- A. Protocol filter
- B. Load balancer
- C. NIDS
- D. Layer 7 firewall

Answer: D

Explanation:

An application-level gateway firewall filters traffic based on user access, group membership, the application or service used, or even the type of resources being transmitted. This type of firewall

operates at the Application layer (Layer 7) of the OSI model.

QUESTION NO: 95

Concurrent use of a firewall, content filtering, antivirus software and an IDS system would be considered components of:

- A. Redundant systems.
- B. Separation of duties.
- C. Layered security.
- D. Application control.

Answer: C

Explanation:

Layered security is the practice of combining multiple mitigating security controls to protect resources and data.

QUESTION NO: 96

A network engineer is designing a secure tunneled VPN. Which of the following protocols would be the MOST secure?

- A. IPsec
- B. SFTP
- C. BGP
- D. PPTP

Answer: A

Explanation:

Layer 2 Tunneling Protocol (L2TP) came about through a partnership between Cisco and Microsoft with the intention of providing a more secure VPN protocol. L2TP is considered to be a more secure option than PPTP, as the IPsec protocol which holds more secure encryption algorithms, is utilized in conjunction with it. It also requires a pre-shared certificate or key. L2TP's strongest level of encryption makes use of 168 bit keys, 3 DES encryption algorithm and requires two levels of authentication.

L2TP has a number of advantages in comparison to PPTP in terms of providing data integrity and authentication of origin verification designed to keep hackers from compromising the system. However, the increased overhead required to manage this elevated security means that it performs at a slower pace than PPTP.

QUESTION NO: 97

Configuring the mode, encryption methods, and security associations are part of which of the following?

- A. IPSec
- B. Full disk encryption
- C. 802.1x
- D. PKI

Answer: A

Explanation:

IPSec can operate in tunnel mode or transport mode. It uses symmetric cryptography to provide encryption security. Furthermore, it makes use of Internet Security Association and Key Management Protocol (ISAKMP).

QUESTION NO: 98

A company's legacy server requires administration using Telnet. Which of the following protocols could be used to secure communication by offering encryption at a lower OSI layer? (Select TWO).

- A. IPv6
- B. SFTP
- C. IPSec
- D. SSH
- E. IPv4

Answer: A,C

Explanation:

Telnet supports IPv6 connections.

IPv6 is the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec is a compulsory component for IPv6.

IPsec operates at Layer 3 of the OSI model, whereas Telnet operates at Layer 7.

QUESTION NO: 99

A network administrator needs to provide daily network usage reports on all layer 3 devices without compromising any data while gathering the information. Which of the following would be configured to provide these reports?

- A. SNMP
- B. SNMPv3
- C. ICMP
- D. SSH

Answer: B

Explanation:

Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

QUESTION NO: 100

Matt, a security administrator, wants to configure all the switches and routers in the network in order to securely monitor their status. Which of the following protocols would he need to configure on each device?

- A. SMTP
- B. SNMPv3
- C. IPSec
- D. SNMP

Answer: B

Explanation: Currently, SNMP is predominantly used for monitoring and performance management. SNMPv3 defines a secure version of SNMP and also facilitates remote configuration of the SNMP entities.

QUESTION NO: 101

A recent vulnerability scan found that Telnet is enabled on all network devices. Which of the following protocols should be used instead of Telnet?

- A. SCP

- B. SSH
- C. SFTP
- D. SSL

Answer: B

Explanation:

SSH transmits both authentication traffic and data in a secured encrypted form, whereas Telnet transmits both authentication credentials and data in clear text.

QUESTION NO: 102

Which of the following is BEST used as a secure replacement for TELNET?

- A. HTTPS
- B. HMAC
- C. GPG
- D. SSH

Answer: D

Explanation:

SSH transmits both authentication traffic and data in a secured encrypted form, whereas Telnet transmits both authentication credentials and data in clear text.

QUESTION NO: 103

A security analyst needs to logon to the console to perform maintenance on a remote server. Which of the following protocols would provide secure access?

- A. SCP
- B. SSH
- C. SFTP
- D. HTTPS

Answer: B

Explanation:

Secure Shell (SSH) is a tunneling protocol originally used on Unix systems. It's now available for both Unix and Windows environments. SSH is primarily intended for interactive terminal sessions. SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

QUESTION NO: 104

A UNIX administrator would like to use native commands to provide a secure way of connecting to other devices remotely and to securely transfer files. Which of the following protocols could be utilized? (Select TWO).

- A. RDP
- B. SNMP
- C. FTP
- D. SCP
- E. SSH

Answer: D,E

Explanation:

SSH is used to establish a command-line, text-only interface connection with a server, router, switch, or similar device over any distance.

Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). SCP is commonly used on Linux and Unix platforms.

QUESTION NO: 105

A network technician is on the phone with the system administration team. Power to the server room was lost and servers need to be restarted. The DNS services must be the first to be restarted. Several machines are powered off. Assuming each server only provides one service, which of the following should be powered on FIRST to establish DNS services?

- A. Bind server
- B. Apache server
- C. Exchange server
- D. RADIUS server

Answer: A

Explanation:

BIND (Berkeley Internet Name Domain) is the most widely used Domain Name System (DNS) software on the Internet. It includes the DNS server component contracted for name daemon. This is the only option that directly involves DNS.

QUESTION NO: 106

When reviewing security logs, an administrator sees requests for the AAAA record of www.comptia.com. Which of the following BEST describes this type of record?

- A. DNSSEC record
- B. IPv4 DNS record
- C. IPSEC DNS record
- D. IPv6 DNS record

Answer: D

Explanation: The AAAA Address record links a FQDN to an IPv6 address.

QUESTION NO: 107

Which of the following should be implemented to stop an attacker from mapping out addresses and/or devices on a network?

- A. Single sign on
- B. IPv6
- C. Secure zone transfers
- D. VoIP

Answer: C

Explanation:

C: A primary DNS server has the "master copy" of a zone, and secondary DNS servers keep copies of the zone for redundancy. When changes are made to zone data on the primary DNS server, these changes must be distributed to the secondary DNS servers for the zone. This is done through zone transfers. If you allow zone transfers to any server, all the resource records in the zone are viewable by any host that can contact your DNS server. Thus you will need to secure the zone transfers to stop an attacker from mapping out your addresses and devices on your network.

QUESTION NO: 108

A security engineer, Joe, has been asked to create a secure connection between his mail server and the mail server of a business partner. Which of the following protocol would be MOST appropriate?

- A. HTTPS

- B. SSH
- C. FTP
- D. TLS

Answer: D

Explanation: Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key. The TLS protocol allows client-server applications to communicate across a network in a way designed to prevent eavesdropping and tampering.

QUESTION NO: 109

Which of the following protocols is used to authenticate the client and server's digital certificate?

- A. PEAP
- B. DNS
- C. TLS
- D. ICMP

Answer: C

Explanation:

Transport Layer Security (TLS) is a cryptographic protocol designed to provide communications security over a computer network. It uses X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom it is communicating, and to exchange a symmetric key.

QUESTION NO: 110

An administrator configures all wireless access points to make use of a new network certificate authority. Which of the following is being used?

- A. WEP
- B. LEAP
- C. EAP-TLS
- D. TKIP

Answer: C

Explanation:

The majority of the EAP-TLS implementations require client-side X.509 certificates without giving the option to disable the requirement.

QUESTION NO: 111

An achievement in providing worldwide Internet security was the signing of certificates associated with which of the following protocols?

- A. TCP/IP
- B. SSL
- C. SCP
- D. SSH

Answer: B

Explanation:

SSL (Secure Sockets Layer) is used for establishing an encrypted link between two computers, typically a web server and a browser. SSL is used to enable sensitive information such as login credentials and credit card numbers to be transmitted securely.

QUESTION NO: 112

Which of the following is the MOST secure protocol to transfer files?

- A. FTP
- B. FTPS
- C. SSH
- D. TELNET

Answer: B

Explanation:

FTPS refers to FTP Secure, or FTP SSL. It is a secure variation of File Transfer Protocol (FTP).

QUESTION NO: 113

FTP/S uses which of the following TCP ports by default?

- A. 20 and 21
- B. 139 and 445
- C. 443 and 22
- D. 989 and 990

Answer: D

Explanation: FTPS uses ports 989 and 990.

QUESTION NO: 114

Which of the following protocols allows for secure transfer of files? (Select TWO).

- A. ICMP
- B. SNMP
- C. SFTP
- D. SCP
- E. TFTP

Answer: C,D

Explanation:

Standard FTP is a protocol often used to move files between one system and another either over the Internet or within private networks. SFTP is a secured alternative to standard FTP.

Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).

QUESTION NO: 115

After a network outage, a PC technician is unable to ping various network devices. The network administrator verifies that those devices are working properly and can be accessed securely.

Which of the following is the MOST likely reason the PC technician is unable to ping those devices?

- A. ICMP is being blocked
- B. SSH is not enabled
- C. DNS settings are wrong
- D. SNMP is not configured properly

Answer: A

Explanation:

ICMP is a protocol that is commonly used by tools such as ping, traceroute, and pathping. ICMP offers no information If ICMP request queries go unanswered, or ICMP replies are lost or blocked.

QUESTION NO: 116

A security administrator wishes to change their wireless network so that IPSec is built into the protocol and NAT is no longer required for address range extension. Which of the following protocols should be used in this scenario?

- A. WPA2
- B. WPA
- C. IPv6
- D. IPv4

Answer: C

Explanation:

IPSec security is built into IPv6.

QUESTION NO: 117

A system administrator attempts to ping a hostname and the response is 2001:4860:0:2001::68.

Which of the following replies has the administrator received?

- A. The loopback address
- B. The local MAC address
- C. IPv4 address
- D. IPv6 address

Answer: D

Explanation:

IPv6 addresses are 128-bits in length. An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:). The hexadecimal digits are case-insensitive, but IETF recommendations suggest the use of lower case letters. The full representation of eight 4-digit groups may be simplified by several techniques, eliminating parts of the representation.

QUESTION NO: 118

Which of the following protocols is used by IPv6 for MAC address resolution?

- A. NDP

- B. ARP
- C. DNS
- D. NCP

Answer: A

Explanation:

The Neighbor Discovery Protocol (NDP) is a protocol in the Internet protocol suite used with Internet Protocol Version 6 (IPv6).

QUESTION NO: 119

Which of the following protocols allows for the LARGEST address space?

- A. IPX
- B. IPv4
- C. IPv6
- D. Appletalk

Answer: C

Explanation:

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared with 32 bits in IPv4.

QUESTION NO: 120

Pete, a network administrator, is implementing IPv6 in the DMZ. Which of the following protocols must he allow through the firewall to ensure the web servers can be reached via IPv6 from an IPv6 enabled Internet host?

- A. TCP port 443 and IP protocol 46
- B. TCP port 80 and TCP port 443
- C. TCP port 80 and ICMP
- D. TCP port 443 and SNMP

Answer: B

Explanation:

HTTP and HTTPS, which uses TCP port 80 and TCP port 443 respectively, is necessary for Communicating with Web servers. It should therefore be allowed through the firewall.

QUESTION NO: 121

Which of the following ports and protocol types must be opened on a host with a host-based firewall to allow incoming SFTP connections?

- A. 21/UDP
- B. 21/TCP
- C. 22/UDP
- D. 22/TCP

Answer: D

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

QUESTION NO: 122

A network administrator is asked to send a large file containing PII to a business associate.

Which of the following protocols is the BEST choice to use?

- A. SSH
- B. SFTP
- C. SMTP
- D. FTP

Answer: B

Explanation:

SFTP encrypts authentication and data traffic between the client and server by making use of SSH to provide secure FTP communications. As a result, SFTP offers protection for both the authentication traffic and the data transfer taking place between a client and server.

QUESTION NO: 123

Which of the following is a difference between TFTP and FTP?

- A. TFTP is slower than FTP.
- B. TFTP is more secure than FTP.
- C. TFTP utilizes TCP and FTP uses UDP.

D. TFTP utilizes UDP and FTP uses TCP.

Answer: D

Explanation:

FTP employs TCP ports 20 and 21 to establish and maintain client-to-server communications, whereas TFTP makes use of UDP port 69.

QUESTION NO: 124

Which of the following is the default port for TFTP?

- A. 20
- B. 69
- C. 21
- D. 68

Answer: B

Explanation:

TFTP makes use of UDP port 69.

QUESTION NO: 125

A network consists of various remote sites that connect back to two main locations. Pete, the security administrator, needs to block TELNET access into the network. Which of the following, by default, would be the BEST choice to accomplish this goal?

- A. Block port 23 on the L2 switch at each remote site
- B. Block port 23 on the network firewall
- C. Block port 25 on the L2 switch at each remote site
- D. Block port 25 on the network firewall

Answer: B

Explanation:

Telnet is a terminal-emulation network application that supports remote connectivity for executing commands and running applications but doesn't support transfer of files. Telnet uses TCP port 23. Because it's a clear text protocol and service, it should be avoided and replaced with SSH.

QUESTION NO: 126

A security analyst noticed a colleague typing the following command:

`Telnet some-host 443`

Which of the following was the colleague performing?

- A.** A hacking attempt to the some-host web server with the purpose of achieving a distributed denial of service attack.
- B.** A quick test to see if there is a service running on some-host TCP/443, which is being routed correctly and not blocked by a firewall.
- C.** Trying to establish an insecure remote management session. The colleague should be using SSH or terminal services instead.
- D.** A mistaken port being entered because telnet servers typically do not listen on port 443.

Answer: B

Explanation:

B: The Telnet program parameters are: telnet <hostname> <port>

<hostname> is the name or IP address of the remote server to connect to.

<port> is the port number of the service to use for the connection.

TCP port 443 provides the HTTPS (used for secure web connections) service; it is the default SSL port. By running the Telnet some-host 443 command, the security analyst is checking that routing is done properly and not blocked by a firewall.

QUESTION NO: 127

A malicious program modified entries in the LMHOSTS file of an infected system. Which of the following protocols would have been affected by this?

- A.** ICMP
- B.** BGP
- C.** NetBIOS
- D.** DNS

Answer: C

Explanation:

The LMHOSTS file provides a NetBIOS name resolution method that can be used for small networks that do not use a WINS server. NetBIOS has been adapted to run on top of TCP/IP, and is still extensively used for name resolution and registration in Windows-based environments.

QUESTION NO: 128 DRAG DROP

Drag and drop the correct protocol to its default port.

FTP	<input type="text"/>	161
Telnet	<input type="text"/>	22
SMTP	<input type="text"/>	21
SNMP	<input type="text"/>	69
SCP	<input type="text"/>	25
TFTP	<input type="text"/>	23

Answer:

FTP	21	161
Telnet	23	22
SMTP	25	21
SNMP	161	69
SCP	22	25
TFTP	69	23

Explanation:

FTP	21
Telnet	23
SMTP	25
SNMP	161
SCP	22
TFTP	69

FTP uses TCP port 21.

Telnet uses port 23.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

SMTP uses TCP port 25.

Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 42, 45, 51

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION NO: 129

An information bank has been established to store contacts, phone numbers and other records. A UNIX application needs to connect to the index server using port 389. Which of the following authentication services should be used on this port by default?

- A. RADIUS
- B. Kerberos
- C. TACACS+
- D. LDAP

Answer: D

Explanation:

LDAP makes use of port 389.

QUESTION NO: 130

A firewall technician has been instructed to disable all non-secure ports on a corporate firewall. The technician has blocked traffic on port 21, 69, 80, and 137-139. The technician has allowed traffic on ports 22 and 443. Which of the following correctly lists the protocols blocked and allowed?

- A. Blocked: TFTP, HTTP, NetBIOS; Allowed: HTTPS, FTP
- B. Blocked: FTP, TFTP, HTTP, NetBIOS; Allowed: SFTP, SSH, SCP, HTTPS
- C. Blocked: SFTP, TFTP, HTTP, NetBIOS; Allowed: SSH, SCP, HTTPS
- D. Blocked: FTP, HTTP, HTTPS; Allowed: SFTP, SSH, SCP, NetBIOS

Answer: B

Explanation:

The question states that traffic on port 21, 69, 80, and 137-139 is blocked, while ports 22 and 443 are allowed.

Port 21 is used for FTP by default.

Port 69 is used for TFTP.

Port 80 is used for HTTP.

Ports 137-139 are used for NetBIOS.

VMM uses SFTP over default port 22.

Port 22 is used for SSH by default.

SCP runs over TCP port 22 by default.

Port 443 is used for HTTPS.

QUESTION NO: 131

A company has implemented PPTP as a VPN solution. Which of the following ports would need to be opened on the firewall in order for this VPN to function properly? (Select TWO).

A. UDP 1723

B. TCP 500

C. TCP 1723

D. UDP 47

E. TCP 47

Answer: C,D

Explanation:

A PPTP tunnel is instantiated by communication to the peer on TCP port 1723. This TCP connection is then used to initiate and manage a second GRE tunnel to the same peer. The PPTP GRE packet format is non-standard, including an additional acknowledgement field replacing the typical routing field in the GRE header. However, as in a normal GRE connection, those modified GRE packets are directly encapsulated into IP packets, and seen as IP protocol number 47.

QUESTION NO: 132

After a new firewall has been installed, devices cannot obtain a new IP address. Which of the following ports should Matt, the security administrator, open on the firewall?

A. 25

B. 68

C. 80

D. 443

Answer: B

Explanation:

The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for distributing IP addresses for interfaces and services. DHCP makes use of port 68.

QUESTION NO: 133

A security administrator has configured FTP in passive mode. Which of the following ports should the security administrator allow on the firewall by default?

- A. 20
- B. 21
- C. 22
- D. 23

Answer: B

Explanation:

When establishing an FTP session, clients start a connection to an FTP server that listens on TCP port 21 by default.

QUESTION NO: 134

Which of the following ports is used for SSH, by default?

- A. 23
- B. 32
- C. 12
- D. 22

Answer: D

Explanation:

Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

QUESTION NO: 135

By default, which of the following uses TCP port 22? (Select THREE).

- A. FTPS
- B. STELNET
- C. TLS
- D. SCP
- E. SSL
- F. HTTPS
- G. SSH
- H. SFTP

Answer: D,G,H

Explanation:

G: Secure Shell (SSH) is a cryptographic network protocol for securing data communication. It establishes a secure channel over an insecure network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login, remote command execution, but any network service can be secured with SSH. SSH uses port 22.

D: SCP stands for Secure Copy. SCP is used to securely copy files over a network. SCP uses SSH to secure the connection and therefore uses port 22.

H: SFTP stands for stands for Secure File Transfer Protocol and is used for transferring files using FTP over a secure network connection. SFTP uses SSH to secure the connection and therefore uses port 22.

QUESTION NO: 136

Pete needs to open ports on the firewall to allow for secure transmission of files. Which of the following ports should be opened on the firewall?

- A. TCP 23
- B. UDP 69
- C. TCP 22
- D. TCP 21

Answer: C

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).

QUESTION NO: 137

Which of the following uses port 22 by default? (Select THREE).

- A. SSH
- B. SSL
- C. TLS
- D. SFTP
- E. SCP
- F. FTPS
- G. SMTP
- H. SNMP

Answer: A,D,E

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

QUESTION NO: 138

Which of the following ports should be used by a system administrator to securely manage a remote server?

- A. 22
- B. 69
- C. 137
- D. 445

Answer: A

Explanation:

Secure Shell (SSH) is a more secure replacement for Telnet, rlogin, rsh, and rcp. SSH can be called a remote access or remote terminal solution. SSH offers a means by which a command-line, text-only interface connection with a server, router, switch, or similar device can be established over any distance. SSH makes use of TCP port 22.

QUESTION NO: 139

Which of the following ports is used to securely transfer files between remote UNIX systems?

- A. 21
- B. 22
- C. 69
- D. 445

Answer: B

Explanation:

SCP copies files securely between hosts on a network. It uses SSH for data transfer, and uses the same authentication and provides the same security as SSH. Unlike RCP, SCP will ask for passwords or passphrases if they are needed for authentication.

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

QUESTION NO: 140

Which of the following secure file transfer methods uses port 22 by default?

- A. FTPS
- B. SFTP
- C. SSL
- D. S/MIME

Answer: B

Explanation:

SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.

QUESTION NO: 141

During the analysis of a PCAP file, a security analyst noticed several communications with a remote server on port 53. Which of the following protocol types is observed in this traffic?

- A. FTP
- B. DNS
- C. Email
- D. NetBIOS

Answer: B

Explanation:

DNS (Domain Name System) uses port 53.

QUESTION NO: 142

A security technician needs to open ports on a firewall to allow for domain name resolution.

Which of the following ports should be opened? (Select TWO).

- A. TCP 21
- B. TCP 23
- C. TCP 53
- D. UDP 23
- E. UDP 53

Answer: C,E

Explanation:

DNS uses TCP and UDP port 53. TCP port 53 is used for zone transfers, whereas UDP port 53 is used for queries.

QUESTION NO: 143

A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

- A. HTTP
- B. DHCP
- C. DNS
- D. NetBIOS

Answer: C

Explanation:

DNS links IP addresses and human-friendly fully qualified domain names (FQDNs), which are made up of the Top-level domain (TLD), the registered domain name, and the Subdomain or hostname.

Therefore, if the DNS ports are blocked websites will not be reachable.

QUESTION NO: 144

Which of the following ports would be blocked if Pete, a security administrator, wants to deny access to websites?

- A. 21
- B. 25
- C. 80
- D. 3389

Answer: C

Explanation:

Port 80 is used by HTTP, which is the foundation of data communication for the World Wide Web.

QUESTION NO: 145

A technician is unable to manage a remote server. Which of the following ports should be opened on the firewall for remote server management? (Select TWO).

- A. 22
- B. 135
- C. 137
- D. 143
- E. 443
- F. 3389

Answer: A,F

Explanation:

A secure remote administration solution and Remote Desktop protocol is required.

Secure Shell (SSH) is a secure remote administration solution and makes use of TCP port 22.

Remote Desktop Protocol (RDP) uses TCP port 3389.

QUESTION NO: 146

Ann, a technician, is attempting to establish a remote terminal session to an end user's computer using Kerberos authentication, but she cannot connect to the destination machine. Which of the following default ports should Ann ensure is open?

- A. 22
- B. 139

- C. 443
- D. 3389

Answer: D

Explanation:

Remote Desktop Protocol (RDP) uses TCP port 3389.

QUESTION NO: 147

Which of the following protocols operates at the HIGHEST level of the OSI model?

- A. ICMP
- B. IPSec
- C. SCP
- D. TCP

Answer: C

Explanation:

SCP (Secure Copy) uses SSH (Secure Shell). SSH runs in the application layer (layer 7) of the OSI model.

QUESTION NO: 148

Which of the following allows Pete, a security technician, to provide the MOST secure wireless implementation?

- A. Implement WPA
- B. Disable SSID
- C. Adjust antenna placement
- D. Implement WEP

Answer: A

Explanation: Of the options supplied, WiFi Protected Access (WPA) is the most secure and is the replacement for WEP.

QUESTION NO: 149

A malicious user is sniffing a busy encrypted wireless network waiting for an authorized client to

connect to it. Only after an authorized client has connected and the hacker was able to capture the client handshake with the AP can the hacker begin a brute force attack to discover the encryption key. Which of the following attacks is taking place?

- A. IV attack
- B. WEP cracking
- C. WPA cracking
- D. Rogue AP

Answer: C

Explanation:

There are three steps to penetrating a WPA-protected network.

Sniffing

Parsing

Attacking

QUESTION NO: 150

Which of the following is a step in deploying a WPA2-Enterprise wireless network?

- A. Install a token on the authentication server
- B. Install a DHCP server on the authentication server
- C. Install an encryption key on the authentication server
- D. Install a digital certificate on the authentication server

Answer: D

Explanation:

When setting up a wireless network, you'll find two very different modes of Wi-Fi Protected Access (WPA) security, which apply to both the WPA and WPA2 versions.

The easiest to setup is the Personal mode, technically called the Pre-Shared Key (PSK) mode. It doesn't require anything beyond the wireless router or access points (APs) and uses a single passphrase or password for all users/devices.

The other is the Enterprise mode—which should be used by businesses and organizations—and is also known as the RADIUS, 802.1X, 802.11i, or EAP mode. It provides better security and key management, and supports other enterprise-type functionality, such as VLANs and NAP.

However, it requires an external authentication server, called a Remote Authentication Dial In User Service (RADIUS) server to handle the 802.1X authentication of users.

To help you better understand the process of setting up WPA/WPA2-Enterprise and 802.1X, here's the basic overall steps:

Choose, install, and configure a RADIUS server, or use a hosted service.

Create a certificate authority (CA), so you can issue and install a digital certificate onto the RADIUS server, which may be done as a part of the RADIUS server installation and configuration. Alternatively, you could purchase a digital certificate from a public CA, such as GoDaddy or Verisign, so you don't have to install the server certificate on all the clients. If using EAP-TLS, you'd also create digital certificates for each end-user.

On the server, populate the RADIUS client database with the IP address and shared secret for each AP.

On the server, populate user data with usernames and passwords for each end-user.

On each AP, configure the security for WPA/WPA2-Enterprise and input the RADIUS server IP address and the shared secret you created for that particular AP.

On each Wi-Fi computer and device, configure the security for WPA/WPA2-Enterprise and set the 802.1X authentication settings.

QUESTION NO: 151

A security administrator must implement a wireless security system, which will require users to enter a 30 character ASCII password on their accounts. Additionally the system must support 3DS wireless encryption.

Which of the following should be implemented?

- A. WPA2-CCMP with 802.1X
- B. WPA2-PSK
- C. WPA2-CCMP
- D. WPA2-Enterprise

Answer: D

Explanation:

D: WPA-Enterprise is also referred to as WPA-802.1X mode, and sometimes just WPA (as opposed to WPA-PSK), this is designed for enterprise networks and requires a RADIUS authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). Various kinds of the Extensible Authentication Protocol (EAP) are used for authentication. RADIUS can be managed centrally, and the servers that allow access to a network can verify with a RADIUS server whether an incoming caller is authorized. Thus the RADIUS server can perform all authentications. This will require users to use their passwords on their user accounts.

QUESTION NO: 152

Configuring key/value pairs on a RADIUS server is associated with deploying which of the following?

- A. WPA2-Enterprise wireless network
- B. DNS secondary zones
- C. Digital certificates
- D. Intrusion detection system

Answer: A

Explanation:

WPA2-Enterprise is designed for enterprise networks and requires a RADIUS authentication server.

QUESTION NO: 153

A security administrator must implement a network authentication solution which will ensure encryption of user credentials when users enter their username and password to authenticate to the network.

Which of the following should the administrator implement?

- A. WPA2 over EAP-TTLS
- B. WPA-PSK
- C. WPA2 with WPS
- D. WEP over EAP-PEAP

Answer: D

Explanation:

D: Wired Equivalent Privacy (WEP) is designed to provide security equivalent to that of a wired network. WEP has vulnerabilities and isn't considered highly secure. Extensible Authentication Protocol (EAP) provides a framework for authentication that is often used with wireless networks. Among the five EAP types adopted by the WPA/ WPA2 standard are EAP-TLS, EAP-PSK, EAP-MD5, as well as LEAP and PEAP.

PEAP is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication, and uses server-side public key certificates to authenticate the server. It then creates an encrypted TLS tunnel between the client and the authentication server. In most configurations, the keys for this encryption are transported using the server's public key. The ensuing exchange of authentication information inside the tunnel to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

QUESTION NO: 154

Which of the following BEST describes the weakness in WEP encryption?

- A.** The initialization vector of WEP uses a crack-able RC4 encryption algorithm. Once enough packets are captured an XOR operation can be performed and the asymmetric keys can be derived.
- B.** The WEP key is stored in plain text and split in portions across 224 packets of random data. Once enough packets are sniffed the IV portion of the packets can be removed leaving the plain text key.
- C.** The WEP key has a weak MD4 hashing algorithm used. A simple rainbow table can be used to generate key possibilities due to MD4 collisions.
- D.** The WEP key is stored with a very small pool of random numbers to make the cipher text. As the random numbers are often reused it becomes easy to derive the remaining WEP key.

Answer: D

Explanation:

WEP is based on RC4, but due to errors in design and implementation, WEP is weak in a number of areas, two of which are the use of a static common key and poor implementation of initiation vectors (IVs). When the WEP key is discovered, the attacker can join the network and then listen in on all other wireless client communications.

QUESTION NO: 155

Which of the following would satisfy wireless network implementation requirements to use mutual authentication and usernames and passwords?

- A.** EAP-MD5
- B.** WEP
- C.** PEAP-MSCHAPv2
- D.** EAP-TLS

Answer: C

Explanation:

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards.

QUESTION NO: 156

Matt, a systems security engineer, is determining which credential-type authentication to use within a planned 802.1x deployment. He is looking for a method that does not require a client certificate, has a server side certificate, and uses TLS tunnels for encryption. Which credential type authentication method BEST fits these requirements?

- A. EAP-TLS
- B. EAP-FAST
- C. PEAP-CHAP
- D. PEAP-MSCHAPv2

Answer: D

Explanation:

PEAP-MS-CHAP v2 is easier to deploy than EAP-TLS or PEAP-TLS because user authentication is accomplished via password-base credentials (user name and password) rather than digital certificates or smart cards. Only servers running Network Policy Server (NPS) or PEAP-MS-CHAP v2 are required to have a certificate.

QUESTION NO: 157

Which of the following means of wireless authentication is easily vulnerable to spoofing?

- A. MAC Filtering
- B. WPA - LEAP
- C. WPA - PEAP
- D. Enabled SSID

Answer: A

Explanation:

Each network interface on your computer or any other networked device has a unique MAC address. These MAC addresses are assigned in the factory, but you can easily change, or "spoof," MAC addresses in software.

Networks can use MAC address filtering, only allowing devices with specific MAC addresses to connect to a network. This isn't a great security tool because people can spoof their MAC addresses.

QUESTION NO: 158

Ann, a sales manager, successfully connected her company-issued smartphone to the wireless network in her office without supplying a username/password combination. Upon disconnecting

from the wireless network, she attempted to connect her personal tablet computer to the same wireless network and could not connect.

Which of the following is MOST likely the reason?

- A. The company wireless is using a MAC filter.
- B. The company wireless has SSID broadcast disabled.
- C. The company wireless is using WEP.
- D. The company wireless is using WPA2.

Answer: A

Explanation:

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

QUESTION NO: 159

After entering the following information into a SOHO wireless router, a mobile device's user reports being unable to connect to the network:

PERMIT 0A: D1: FA. B1: 03: 37

DENY 01: 33: 7F: AB: 10: AB

Which of the following is preventing the device from connecting?

- A. WPA2-PSK requires a supplicant on the mobile device.
- B. Hardware address filtering is blocking the device.
- C. TCP/IP Port filtering has been implemented on the SOHO router.
- D. IP address filtering has disabled the device from connecting.

Answer: B

Explanation:

MAC filtering allows you to include or exclude computers and devices based on their MAC address.

QUESTION NO: 160

A security analyst has been tasked with securing a guest wireless network. They recommend the company use an authentication server but are told the funds are not available to set this up.

Which of the following BEST allows the analyst to restrict user access to approved devices?

- A. Antenna placement
- B. Power level adjustment
- C. Disable SSID broadcasting
- D. MAC filtering

Answer: D

Explanation:

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

QUESTION NO: 161

If you don't know the MAC address of a Linux-based machine, what command-line utility can you use to ascertain it?

- A. macconfig
- B. ifconfig
- C. ipconfig
- D. config

Answer: B

Explanation:

To find MAC address of a Unix/Linux workstation, use ifconfig or ip a.

QUESTION NO: 162

An organization does not want the wireless network name to be easily discovered. Which of the following software features should be configured on the access points?

- A. SSID broadcast
- B. MAC filter
- C. WPA2
- D. Antenna placement

Answer: A

Explanation:

Numerous networks broadcast their name (known as an SSID broadcast) to reveal their presence.

QUESTION NO: 163

A security architect wishes to implement a wireless network with connectivity to the company's internal network. Before they inform all employees that this network is being put in place, the architect wants to roll it out to a small test segment. Which of the following allows for greater secrecy about this network during this initial phase of implementation?

- A. Disabling SSID broadcasting
- B. Implementing WPA2 - TKIP
- C. Implementing WPA2 - CCMP
- D. Filtering test workstations by MAC address

Answer: A

Explanation:

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

QUESTION NO: 164

While previously recommended as a security measure, disabling SSID broadcast is not effective against most attackers because network SSIDs are:

- A. no longer used to authenticate to most wireless networks.
- B. contained in certain wireless packets in plaintext.
- C. contained in all wireless broadcast packets by default.
- D. no longer supported in 802.11 protocols.

Answer: B

Explanation:

The SSID is still required for directing packets to and from the base station, so it can be discovered using a wireless packet sniffer.

QUESTION NO: 165

A company provides secure wireless Internet access for visitors and vendors working onsite. Some of the vendors using older technology report that they are unable to access the wireless

network after entering the correct network information. Which of the following is the MOST likely reason for this issue?

- A. The SSID broadcast is disabled.
- B. The company is using the wrong antenna type.
- C. The MAC filtering is disabled on the access point.
- D. The company is not using strong enough encryption.

Answer: A

Explanation:

When the SSID is broadcast, any device with an automatic detect and connect feature is able to see the network and can initiate a connection with it. The fact that they cannot access the network means that they are unable to see it.

QUESTION NO: 166

Which of the following best practices makes a wireless network more difficult to find?

- A. Implement MAC filtering
- B. Use WPA2-PSK
- C. Disable SSID broadcast
- D. Power down unused WAPs

Answer: C

Explanation:

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

QUESTION NO: 167

Jane, the security administrator, sets up a new AP but realizes too many outsiders are able to connect to that AP and gain unauthorized access. Which of the following would be the BEST way to mitigate this issue and still provide coverage where needed? (Select TWO).

- A. Disable the wired ports
- B. Use channels 1, 4 and 7 only
- C. Enable MAC filtering
- D. Disable SSID broadcast

E. Switch from 802.11a to 802.11b

Answer: C,D

Explanation: Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

QUESTION NO: 168

Which of the following wireless security technologies continuously supplies new keys for WEP?

- A. TKIP
- B. Mac filtering
- C. WPA2
- D. WPA

Answer: A

Explanation:

TKIP is a suite of algorithms that works as a "wrapper" to WEP, which allows users of legacy WLAN equipment to upgrade to TKIP without replacing hardware. TKIP uses the original WEP programming but "wraps" additional code at the beginning and end to encapsulate and modify it.

QUESTION NO: 169

A network administrator has been tasked with securing the WLAN. Which of the following cryptographic products would be used to provide the MOST secure environment for the WLAN?

- A. WPA2 CCMP
- B. WPA
- C. WPA with MAC filtering
- D. WPA2 TKIP

Answer: A

Explanation:

CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the WEP protocol and TKIP protocol of WPA. CCMP provides the following security

services:

Data confidentiality; ensures only authorized parties can access the information

Authentication; provides proof of genuineness of the user

Access control in conjunction with layer management

Because CCMP is a block cipher mode using a 128-bit key, it is secure against attacks to the 264 steps of operation.

QUESTION NO: 170

An access point has been configured for AES encryption but a client is unable to connect to it. Which of the following should be configured on the client to fix this issue?

- A. WEP
- B. CCMP
- C. TKIP
- D. RC4

Answer: B

Explanation:

CCMP is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard.

QUESTION NO: 171

A security administrator wishes to increase the security of the wireless network. Which of the following BEST addresses this concern?

- A. Change the encryption from TKIP-based to CCMP-based.
- B. Set all nearby access points to operate on the same channel.
- C. Configure the access point to use WEP instead of WPA2.
- D. Enable all access points to broadcast their SSIDs.

Answer: A

Explanation:

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

QUESTION NO: 172

The security administrator has been tasked to update all the access points to provide a more secure connection. All access points currently use WPA TKIP for encryption. Which of the following would be configured to provide more secure connections?

- A. WEP
- B. WPA2 CCMP
- C. Disable SSID broadcast and increase power levels
- D. MAC filtering

Answer: B

Explanation:

CCMP makes use of 128-bit AES encryption with a 48-bit initialization vector. This initialization vector makes cracking a bit more difficult.

QUESTION NO: 173

A system administrator wants to enable WPA2 CCMP. Which of the following is the only encryption used?

- A. RC4
- B. DES
- C. 3DES
- D. AES

Answer: D

Explanation:

Cipher Block Chaining Message Authentication Code Protocol (CCMP) makes use of 128-bit AES encryption with a 48-bit initialization vector.

QUESTION NO: 174

Jane, an administrator, needs to make sure the wireless network is not accessible from the parking area of their office. Which of the following would BEST help Jane when deploying a new access point?

- A. Placement of antenna
- B. Disabling the SSID
- C. Implementing WPA2
- D. Enabling the MAC filtering

Answer: A

Explanation:

You should try to avoid placing access points near metal (which includes appliances) or near the ground. Placing them in the center of the area to be served and high enough to get around most obstacles is recommended. On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

QUESTION NO: 175

A security team has identified that the wireless signal is broadcasting into the parking lot. To reduce the risk of an attack against the wireless network from the parking lot, which of the following controls should be used? (Select TWO).

- A. Antenna placement
- B. Interference
- C. Use WEP
- D. Single Sign on
- E. Disable the SSID
- F. Power levels

Answer: A,F

Explanation:

Placing the antenna in the correct position is crucial. You can then adjust the power levels to exclude the parking lot.

QUESTION NO: 176

Which of the following would Pete, a security administrator, do to limit a wireless signal from penetrating the exterior walls?

- A. Implement TKIP encryption
- B. Consider antenna placement
- C. Disable the SSID broadcast
- D. Disable WPA

Answer: B

Explanation: Cinderblock walls, metal cabinets, and other barriers can reduce signal strength significantly. Therefore, antenna placement is critical.

QUESTION NO: 177

Ann, a security administrator, has concerns regarding her company's wireless network. The network is open and available for visiting prospective clients in the conference room, but she notices that many more devices are connecting to the network than should be.

Which of the following would BEST alleviate Ann's concerns with minimum disturbance of current functionality for clients?

- A. Enable MAC filtering on the wireless access point.
- B. Configure WPA2 encryption on the wireless access point.
- C. Lower the antenna's broadcasting power.
- D. Disable SSID broadcasting.

Answer: C

Explanation:

Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

QUESTION NO: 178

After reviewing the firewall logs of her organization's wireless APs, Ann discovers an unusually high amount of failed authentication attempts in a particular segment of the building. She remembers that a new business moved into the office space across the street. Which of the following would be the BEST option to begin addressing the issue?

- A. Reduce the power level of the AP on the network segment
- B. Implement MAC filtering on the AP of the affected segment
- C. Perform a site survey to see what has changed on the segment
- D. Change the WPA2 encryption key of the AP in the affected segment

Answer: A

Explanation:

Some access points include power level controls that allow you to reduce the amount of output provided if the signal is traveling too far.

QUESTION NO: 179

An administrator wants to establish a WiFi network using a high gain directional antenna with a narrow radiation pattern to connect two buildings separated by a very long distance. Which of the following antennas would be BEST for this situation?

- A. Dipole
- B. Yagi
- C. Sector
- D. Omni

Answer: B

Explanation:

A Yagi-Uda antenna, commonly known simply as a Yagi antenna, is a directional antenna consisting of multiple parallel dipole elements in a line, usually made of metal rods. It consists of a single driven element connected to the transmitter or receiver with a transmission line, and additional parasitic elements: a so-called reflector and one or more directors. The reflector element is slightly longer than the driven dipole, whereas the directors are a little shorter. This design achieves a very substantial increase in the antenna's directionality and gain compared to a simple dipole.

QUESTION NO: 180

A company has recently implemented a high density wireless system by having a junior technician install two new access points for every access point already deployed. Users are now reporting random wireless disconnections and slow network connectivity. Which of the following is the MOST likely cause?

- A. The old APs use 802.11a
- B. Users did not enter the MAC of the new APs
- C. The new APs use MIMO
- D. A site survey was not conducted

Answer: D

Explanation:

To test the wireless AP placement, a site survey should be performed.

QUESTION NO: 181

A Windows-based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?

- A. Kill all system processes
- B. Enable the firewall
- C. Boot from CD/USB
- D. Disable the network connection

Answer: C

Explanation:

Antivirus companies frequently create boot discs you can use to scan and repair your computer. These tools can be burned to a CD or DVD or installed onto a USB drive. You can then restart your computer and boot from the removable media. A special antivirus environment will load where your computer can be scanned and repaired.

Incorrect Options:

- A: Kill all system processes will stop system processes, and could have a negative effect on the system. It is not the BEST way to run the malware scanner
- B: The basic purpose of a firewall is to isolate one network from another. It is not the BEST way to run the malware scanner.
- D: Disabling the network connection will not allow for the BEST way to run the malware scanner.

Reference:

<http://www.howtogeek.com/187037/how-to-scan-and-repair-a-badly-infected-computer-from-outside-windows/>

Dulaney, Emmett and Chuck Easton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 342

QUESTION NO: 182

A company administrator has a firewall with an outside interface connected to the Internet and an inside interface connected to the corporate network. Which of the following should the administrator configure to redirect traffic destined for the default HTTP port on the outside interface to an internal server listening on port 8080?

- A. Create a dynamic PAT from port 80 on the outside interface to the internal interface on port 8080

- B.** Create a dynamic NAT from port 8080 on the outside interface to the server IP address on port 80
- C.** Create a static PAT from port 80 on the outside interface to the internal interface on port 8080
- D.** Create a static PAT from port 8080 on the outside interface to the server IP address on port 80

Answer: C

Explanation:

Static PAT translations allow a specific UDP or TCP port on a global address to be translated to a specific port on a local address. In this case, the default HTTP port (80) is the global address to be translated, and port 8080 is the specific port on a local address.

Incorrect Options:

A: Dynamic PAT is not a valid type of PAT.

B: Dynamic NAT translates a group of real addresses to a pool of mapped addresses that are routable on the destination network. The question also states that the internal server is listening on port 8080.

D: The question states that the internal server is listening on port 8080.

Reference:

http://www.cisco.com/c/en/us/td/docs/security/asa/asa82/configuration/guide/config/nat_staticpat.html

QUESTION NO: 183

An overseas branch office within a company has many more technical and non-technical security incidents than other parts of the company. Which of the following management controls should be introduced to the branch office to improve their state of security?

- A.** Initial baseline configuration snapshots
- B.** Firewall, IPS and network segmentation
- C.** Event log analysis and incident response
- D.** Continuous security monitoring processes

Answer: D

Explanation:

Continuous monitoring may involve regular measurements of network traffic levels, routine evaluations for regulatory compliance, and checks of network security device configurations. It also points toward the never-ending review of what resources a user actually accesses, which is critical for preventing insider threats.

Incorrect Options:

A: An initial baseline configuration snapshot would allow for the standardized minimal level of security that all systems in an organization must comply with to be enforced. This will not cover the non-technical security incidents.

B: A Firewall, IPS and network segmentation will offer technical protection, but not non-technical security protection.

C: Event log analysis and incident response will not cover the non-technical security incidents.

Reference:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 154.

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 207, 208

QUESTION NO: 184

Which of the following is a directional antenna that can be used in point-to-point or point-to-multi-point WiFi communication systems? (Select TWO).

- A. Backfire
- B. Dipole
- C. Omni
- D. PTZ
- E. Dish

Answer: A,E

Explanation:

Both the Backfire and the Dish antennae are high gain antenna types that transmit a narrow beam of signal. It can therefore be used as a point-to-point antenna over short distances, but as point-to-multi-point antenna over longer distances.

QUESTION NO: 185

Which of the following would be MOST appropriate to secure an existing SCADA system by preventing connections from unauthorized networks?

- A. Implement a HIDS to protect the SCADA system

- B. Implement a Layer 2 switch to access the SCADA system
- C. Implement a firewall to protect the SCADA system
- D. Implement a NIDS to protect the SCADA system

Answer: C

Explanation:

Firewalls manage traffic using filters, which is just a rule or set of rules. A recommended guideline for firewall rules is, "deny by default; allow by exception". This means that if a network connection is not specifically allowed, it will be denied.

QUESTION NO: 186

The common method of breaking larger network address space into smaller networks is known as:

- A. subnetting.
- B. phishing.
- C. virtualization.
- D. packet filtering.

Answer: A

Explanation:

Subnetting is a dividing process used on networks to divide larger groups of hosts into smaller collections.

QUESTION NO: 187

While securing a network it is decided to allow active FTP connections into the network. Which of the following ports MUST be configured to allow active FTP connections? (Select TWO).

- A. 20
- B. 21
- C. 22
- D. 68
- E. 69

Answer: A,B

Explanation:

FTP (File Transfer Protocol) makes use of ports 20 and 21

QUESTION NO: 188

An administrator needs to secure a wireless network and restrict access based on the hardware address of the device. Which of the following solutions should be implemented?

- A. Use a stateful firewall
- B. Enable MAC filtering
- C. Upgrade to WPA2 encryption
- D. Force the WAP to use channel 1

Answer: B

Explanation:

MAC addresses are also known as an Ethernet hardware address (EHA), hardware address or physical address. Enabling MAC filtering would allow for a WAP to restrict or allow access based on the hardware address of the device.

QUESTION NO: 189

A security administrator must implement a firewall rule to allow remote employees to VPN onto the company network. The VPN concentrator implements SSL VPN over the standard HTTPS port. Which of the following is the MOST secure ACL to implement at the company's gateway firewall?

- A. PERMIT TCP FROM ANY 443 TO 199.70.5.25 443
- B. PERMIT TCP FROM ANY ANY TO 199.70.5.23 ANY
- C. PERMIT TCP FROM 199.70.5.23 ANY TO ANY ANY
- D. PERMIT TCP FROM ANY 1024-65535 TO 199.70.5.23 443

Answer: D

Explanation:

The default HTTPS port is port 443. When configuring SSL VPN you can change the default port for HTTPS to a port within the 1024-65535 range. This ACL will allow traffic from VPNs using the 1024-65535 port range to access the company network via company's gateway firewall on port 443.

QUESTION NO: 190

It is MOST important to make sure that the firewall is configured to do which of the following?

- A. Alert management of a possible intrusion.
- B. Deny all traffic and only permit by exception.

- C. Deny all traffic based on known signatures.
- D. Alert the administrator of a possible intrusion.

Answer: B

Explanation:

Firewalls manage traffic using filters, which is just a rule or set of rules. A recommended guideline for firewall rules is, "deny by default; allow by exception".

QUESTION NO: 191

An administrator needs to secure RADIUS traffic between two servers. Which of the following is the BEST solution?

- A. Require IPSec with AH between the servers
- B. Require the message-authenticator attribute for each message
- C. Use MSCHAPv2 with MPPE instead of PAP
- D. Require a long and complex shared secret for the servers

Answer: A

Explanation:

IPsec is used for a secure point-to-point connection traversing an insecure network such as the Internet. Authentication Header (AH) is a primary IPsec protocol that provides authentication of the sender's data.

QUESTION NO: 192

Ann, the Chief Information Officer (CIO) of a company, sees cloud computing as a way to save money while providing valuable services. She is looking for a cost-effective solution to assist in capacity planning as well as visibility into the performance of the network. Which of the following cloud technologies should she look into?

- A. IaaS
- B. MaaS
- C. SaaS
- D. PaaS

Answer: B

Explanation:

Monitoring-as-a-service (MaaS) is a cloud delivery model that falls under anything as a service (XaaS). MaaS allows for the deployment of monitoring functionalities for several other services

and applications within the cloud.

QUESTION NO: 193

Ann, the network administrator, is receiving reports regarding a particular wireless network in the building. The network was implemented for specific machines issued to the developer department, but the developers are stating that they are having connection issues as well as slow bandwidth. Reviewing the wireless router's logs, she sees that devices not belonging to the developers are connecting to the access point. Which of the following would BEST alleviate the developer's reports?

- A.** Configure the router so that wireless access is based upon the connecting device's hardware address.
- B.** Modify the connection's encryption method so that it is using WEP instead of WPA2.
- C.** Implement connections via secure tunnel with additional software on the developer's computers.
- D.** Configure the router so that its name is not visible to devices scanning for wireless networks.

Answer: A

Explanation:

MAC addresses are also known as an Ethernet hardware address (EHA), hardware address or physical address. Enabling MAC filtering would allow for a WAP to restrict or allow access based on the hardware address of the device.

QUESTION NO: 194

An organization recently switched from a cloud-based email solution to an in-house email server. The firewall needs to be modified to allow for sending and receiving email. Which of the following ports should be open on the firewall to allow for email traffic? (Select THREE).

- A.** TCP 22
- B.** TCP 23
- C.** TCP 25
- D.** TCP 53
- E.** TCP 110
- F.** TCP 143
- G.** TCP 445

Answer: C,E,F

Explanation:

Port 25 is used by Simple Mail Transfer Protocol (SMTP) for routing e-mail between mail servers. Port 110 is used for Post Office Protocol v3 (POP3), which is an application-layer Internet standard protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection. Port 143 is used by Internet Message Access Protocol (IMAP) for the management of email messages.

QUESTION NO: 195

A technician wants to securely collect network device configurations and statistics through a scheduled and automated process. Which of the following should be implemented if configuration integrity is most important and a credential compromise should not allow interactive logons?

- A. SNMPv3
- B. TFTP
- C. SSH
- D. TLS

Answer: A

Explanation:

SNMPv3 provides the following security features:

Message integrity--Ensures that a packet has not been tampered with in transit.

Authentication--Determines that the message is from a valid source.

Encryption--Scrambles the content of a packet to prevent it from being learned by an unauthorized source.

QUESTION NO: 196

A security administrator is tasked with ensuring that all devices have updated virus definition files before they are allowed to access network resources. Which of the following technologies would be used to accomplish this goal?

- A. NIDS
- B. NAC
- C. DLP
- D. DMZ
- E. Port Security

Answer: B

Explanation:

Network Access Control (NAC) means controlling access to an environment through strict adherence to and implementation of security policies.

QUESTION NO: 197

The loss prevention department has purchased a new application that allows the employees to monitor the alarm systems at remote locations. However, the application fails to connect to the vendor's server and the users are unable to log in. Which of the following are the MOST likely causes of this issue? (Select TWO).

- A. URL filtering
- B. Role-based access controls
- C. MAC filtering
- D. Port Security
- E. Firewall rules

Answer: A,E

Explanation:

A URL filter is used to block URLs (websites) to prevent users accessing the website.

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:

Block the connection

Allow the connection

Allow the connection only if it is secured

Incorrect Options:

B: Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. Since the sales team needs to save and print reports, they would not be restricted if restrictions were role-based.

C: A MAC filter is a list of authorized wireless client interface MAC addresses that is used by a WAP to block access to all unauthorized devices.

D: Port security works at level 2 of the OSI model and allows an administrator to configure switch ports so that only certain MAC addresses can use the port.

Reference:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 19, 61, 276

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex,

Indianapolis, 2014, p. 157

QUESTION NO: 198

Ann is an employee in the accounting department and would like to work on files from her home computer. She recently heard about a new personal cloud storage service with an easy web interface. Before uploading her work related files into the cloud for access, which of the following is the MOST important security concern Ann should be aware of?

- A. Size of the files
- B. Availability of the files
- C. Accessibility of the files from her mobile device
- D. Sensitivity of the files

Answer: D

Explanation:

Cloud computing has privacy concerns, regulation compliance difficulties, use of open-/closed-source solutions, and adoption of open standards. It is also unsure whether cloud-based data is actually secured (or even securable).

QUESTION NO: 199

An active directory setting restricts querying to only secure connections. Which of the following ports should be selected to establish a successful connection?

- A. 389
- B. 440
- C. 636
- D. 3286

Answer: C

Explanation:

Port 636 is used for secure LDAP (LDAPS).

Incorrect Options:

- A: Port 389 is used for LDAP.
- B: Port 440 is not used for secure Active Directory connections.
- D: Port 3286 is not used for secure Active Directory connections.

Reference:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 147

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION NO: 200

Signed digital certificates used to secure communication with a web server are MOST commonly associated with which of the following ports?

- A. 25
- B. 53
- C. 143
- D. 443

Answer: D

Explanation:

HTTPS authenticates the website and corresponding web server with which one is communicating. HTTPS makes use of port 443.

Incorrect Options:

A: Port 25 is used by Simple Mail Transfer Protocol (SMTP) for routing e-mail between mail servers.

B: Port 53 is used by Domain Name System (DNS).

C: Port 143 is used by Internet Message Access Protocol (IMAP) for the management of email messages.

Reference:

<https://en.wikipedia.org/wiki/HTTPS>

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION NO: 201

An organization has three divisions: Accounting, Sales, and Human Resources. Users in the

Accounting division require access to a server in the Sales division, but no users in the Human Resources division should have access to resources in any other division, nor should any users in the Sales division have access to resources in the Accounting division. Which of the following network segmentation schemas would BEST meet this objective?

- A. Create two VLANS, one for Accounting and Sales, and one for Human Resources.
- B. Create one VLAN for the entire organization.
- C. Create two VLANs, one for Sales and Human Resources, and one for Accounting.
- D. Create three separate VLANS, one for each division.

Answer: D

Explanation:

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

QUESTION NO: 202

A retail store uses a wireless network for its employees to access inventory from anywhere in the store. Due to concerns regarding the aging wireless network, the store manager has brought in a consultant to harden the network. During the site survey, the consultant discovers that the network was using WEP encryption. Which of the following would be the BEST course of action for the consultant to recommend?

- A. Replace the unidirectional antenna at the front of the store with an omni-directional antenna.
- B. Change the encryption used so that the encryption protocol is CCMP-based.
- C. Disable the network's SSID and configure the router to only access store devices based on MAC addresses.
- D. Increase the access point's encryption from WEP to WPA TKIP.

Answer: B

Explanation:

CCMP is the standard encryption protocol for use with the WPA2 standard and is much more secure than the WEP protocol and TKIP protocol of WPA. CCMP provides the following security services:

Data confidentiality; ensures only authorized parties can access the information
Authentication; provides proof of genuineness of the user
Access control in conjunction with layer management

Incorrect Options:

A: The antenna type deals with signal strength and direction. It will not have a bearing on whether technology is older.

C: This option would “cloak” the network, not harden the network.

D: WPA2, which uses CCMP as its standard encryption protocol, more secure than WPA-TKIP.

Reference:

<http://en.wikipedia.org/wiki/CCMP>

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 61, 63

QUESTION NO: 203

A server is configured to communicate on both VLAN 1 and VLAN 12. VLAN 1 communication works fine, but VLAN 12 does not. Which of the following **MUST** happen before the server can communicate on VLAN 12?

- A. The server's network switch port must be enabled for 802.11x on VLAN 12.
- B. The server's network switch port must use VLAN Q-in-Q for VLAN 12.
- C. The server's network switch port must be 802.1q untagged for VLAN 12.
- D. The server's network switch port must be 802.1q tagged for VLAN 12.

Answer: D

Explanation:

802.1q is a standard that defines a system of VLAN tagging for Ethernet frames. The purpose of a tagged port is to pass traffic for multiple VLAN's.

Incorrect Options:

- A: 802.11x provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.
- B: VLAN Q-in-Q allows multiple VLAN tags to be inserted into a single frame.
- C: The purpose an untagged port is to accept traffic for a single VLAN only.

Reference:

https://en.wikipedia.org/wiki/IEEE_802.1Q

https://documentation.meraki.com/zGeneral_Administration/Tools_and_Troubleshooting/Fundamentals_of_802.1Q_VLAN_Tagging

https://en.wikipedia.org/wiki/IEEE_802.1X

https://en.wikipedia.org/wiki/IEEE_802.1ad

Topic 2, Compliance and Operational Security

QUESTION NO: 204

Three of the primary security control types that can be implemented are.

- A. Supervisory, subordinate, and peer.
- B. Personal, procedural, and legal.
- C. Operational, technical, and management.
- D. Mandatory, discretionary, and permanent.

Answer: C

Explanation:

The National Institute of Standards and Technology (NIST) places controls into various types. The control types fall into three categories: Management, Operational, and Technical.

QUESTION NO: 205

Which of the following technical controls is BEST used to define which applications a user can install and run on a company issued mobile device?

- A. Authentication
- B. Blacklisting
- C. Whitelisting
- D. Acceptable use policy

Answer: C

Explanation:

White lists are closely related to ACLs and essentially, a white list is a list of items that are allowed.

QUESTION NO: 206

To help prevent unauthorized access to PCs, a security administrator implements screen savers that lock the PC after five minutes of inactivity. Which of the following controls is being described in this situation?

- A. Management
- B. Administrative
- C. Technical
- D. Operational

Answer: C

Explanation:

controls such as preventing unauthorized access to PC's and applying screensavers that lock the PC after five minutes of inactivity is a technical control type, the same as Identification and Authentication, Access Control, Audit and Accountability as well as System and Communication Protection.

QUESTION NO: 207

Which of the following is a management control?

- A. Logon banners
- B. Written security policy
- C. SYN attack prevention
- D. Access Control List (ACL)

Answer: B

Explanation:

Management control types include risk assessment, planning, systems and Services Acquisition as well as Certification, Accreditation and Security Assessment; and written security policy falls in this category.

QUESTION NO: 208

Which of the following can result in significant administrative overhead from incorrect reporting?

- A. Job rotation
- B. Acceptable usage policies
- C. False positives
- D. Mandatory vacations

Answer: C

Explanation:

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about. This causes a significant administrative overhead because the reporting is what

results in the false positives.

QUESTION NO: 209

A vulnerability scan is reporting that patches are missing on a server. After a review, it is determined that the application requiring the patch does not exist on the operating system.

Which of the following describes this cause?

- A. Application hardening
- B. False positive
- C. Baseline code review
- D. False negative

Answer: B

Explanation:

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

QUESTION NO: 210

Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

- A. True negatives
- B. True positives
- C. False positives
- D. False negatives

Answer: C

Explanation:

False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

QUESTION NO: 211

Which of the following is an example of a false negative?

- A. The IDS does not identify a buffer overflow.
- B. Anti-virus identifies a benign application as malware.
- C. Anti-virus protection interferes with the normal operation of an application.
- D. A user account is locked out after the user mistypes the password too many times.

Answer: A

Explanation:

With a false negative, you are not alerted to a situation when you should be alerted.

QUESTION NO: 212

A company storing data on a secure server wants to ensure it is legally able to dismiss and prosecute staff who intentionally access the server via Telnet and illegally tamper with customer data. Which of the following administrative controls should be implemented to BEST achieve this?

- A. Command shell restrictions
- B. Restricted interface
- C. Warning banners
- D. Session output pipe to /dev/null

Answer: C

Explanation:

Within Microsoft Windows, you have the ability to put signs (in the form of onscreen pop-up banners) that appear before the login telling similar information—authorized access only, violators will be prosecuted, and so forth. Such banners convey warnings or regulatory information to the user that they must “accept” in order to use the machine or network. You need to make staff aware that they may legally be prosecuted and a message is best given via a banner so that all staff using workstation will get notification.

QUESTION NO: 213

Joe, a security analyst, asks each employee of an organization to sign a statement saying that they understand how their activities may be monitored. Which of the following BEST describes this statement? (Select TWO).

- A. Acceptable use policy
- B. Risk acceptance policy
- C. Privacy policy

- D. Email policy
- E. Security policy

Answer: A,C

Explanation:

Privacy policies define what controls are required to implement and maintain the sanctity of data privacy in the work environment. Privacy policy is a legal document that outlines how data collected is secured. It should encompass information regarding the information the company collects, privacy choices you have based on your account, potential information sharing of your data with other parties, security measures in place, and enforcement.

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

QUESTION NO: 214

Joe, a newly hired employee, has a corporate workstation that has been compromised due to several visits to P2P sites. Joe insisted that he was not aware of any company policy that prohibits the use of such web sites. Which of the following is the BEST method to deter employees from the improper use of the company's information systems?

- A. Acceptable Use Policy
- B. Privacy Policy
- C. Security Policy
- D. Human Resource Policy

Answer: A

Explanation:

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

QUESTION NO: 215

Pete, a security analyst, has been informed that the development team has plans to develop an application which does not meet the company's password policy. Which of the following should Pete do NEXT?

- A. Contact the Chief Information Officer and ask them to change the company password policy so that the application is made compliant.
- B. Tell the application development manager to code the application to adhere to the company's password policy.

- C.** Ask the application development manager to submit a risk acceptance memo so that the issue can be documented.
- D.** Inform the Chief Information Officer of non-adherence to the security policy so that the developers can be reprimanded.

Answer: B

Explanation:

Since the application is violating the security policy it should be coded differently to comply with the password policy.

QUESTION NO: 216

A major security risk with co-mingling of hosts with different security requirements is:

- A.** Security policy violations.
- B.** Zombie attacks.
- C.** Password compromises.
- D.** Privilege creep.

Answer: A

Explanation:

The entire network is only as strong as the weakest host. Thus with the co-mingling of hosts with different security requirements would be risking security policy violations.

QUESTION NO: 217

Which of the following provides the BEST explanation regarding why an organization needs to implement IT security policies?

- A.** To ensure that false positives are identified
- B.** To ensure that staff conform to the policy
- C.** To reduce the organizational risk
- D.** To require acceptable usage of IT systems

Answer: C

Explanation:

Once risks has been identified and assessed then there are five possible actions that should be taken. These are: Risk avoidance, Risk transference, Risk mitigation, Risk deterrence and Risk acceptance. Anytime you engage in steps to reduce risk, you are busy with risk mitigation and implementing IT security policy is a risk mitigation strategy.

QUESTION NO: 218

Which of the following should Pete, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from their company?

- A. Privacy Policy
- B. Least Privilege
- C. Acceptable Use
- D. Mandatory Vacations

Answer: D

Explanation:

A mandatory vacation policy requires all users to take time away from work to refresh. But not only does mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels as well as an opportunity to discover fraud.

QUESTION NO: 219

Two members of the finance department have access to sensitive information. The company is concerned they may work together to steal information. Which of the following controls could be implemented to discover if they are working together?

- A. Least privilege access
- B. Separation of duties
- C. Mandatory access control
- D. Mandatory vacations

Answer: D

Explanation:

A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud. In this case mandatory vacations can prevent the two members from colluding to steal the information that they have access to.

QUESTION NO: 220

Mandatory vacations are a security control which can be used to uncover which of the following?

- A. Fraud committed by a system administrator
- B. Poor password security among users
- C. The need for additional security staff
- D. Software vulnerabilities in vendor code

Answer: A

Explanation:

Mandatory vacations also provide an opportunity to discover fraud apart from the obvious benefits of giving employees a chance to refresh and making sure that others in the company can fill those positions and make the company less dependent on those persons; a sort of replication and duplication at all levels.

QUESTION NO: 221

While rarely enforced, mandatory vacation policies are effective at uncovering:

- A. Help desk technicians with oversight by multiple supervisors and detailed quality control systems.
- B. Collusion between two employees who perform the same business function.
- C. Acts of incompetence by a systems engineer designing complex architectures as a member of a team.
- D. Acts of gross negligence on the part of system administrators with unfettered access to system and no oversight.

Answer: D

Explanation:

Least privilege (privilege reviews) and job rotation is done when mandatory vacations are implemented. Then it will uncover areas where the system administrators neglected to check all users' privileges since the other users must fill in their positions when they are on their mandatory vacation.

QUESTION NO: 222

A company that has a mandatory vacation policy has implemented which of the following controls?

- A. Risk control

- B. Privacy control
- C. Technical control
- D. Physical control

Answer: A

Explanation:

Risk mitigation is done anytime you take steps to reduce risks. Thus mandatory vacation implementation is done as a risk control measure because it is a step that is taken as risk mitigation.

QUESTION NO: 223

Which of the following should Joe, a security manager, implement to reduce the risk of employees working in collusion to embezzle funds from his company?

- A. Privacy Policy
- B. Least Privilege
- C. Acceptable Use
- D. Mandatory Vacations

Answer: D

Explanation:

When one person fills in for another, such as for mandatory vacations, it provides an opportunity to see what the person is doing and potentially uncover any fraud.

QUESTION NO: 224

A company is looking to reduce the likelihood of employees in the finance department being involved with money laundering. Which of the following controls would BEST mitigate this risk?

- A. Implement privacy policies
- B. Enforce mandatory vacations
- C. Implement a security policy
- D. Enforce time of day restrictions

Answer: B

Explanation:

A mandatory vacation policy requires all users to take time away from work to refresh. And in the same time it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfy the need to have replication or duplication at all levels in addition to affording the

company an opportunity to discover fraud for when others do the same job in the absence of the regular staff member then there is transparency.

QUESTION NO: 225

The Chief Security Officer (CSO) is concerned about misuse of company assets and wishes to determine who may be responsible. Which of the following would be the BEST course of action?

- A. Create a single, shared user account for every system that is audited and logged based upon time of use.
- B. Implement a single sign-on application on equipment with sensitive data and high-profile shares.
- C. Enact a policy that employees must use their vacation time in a staggered schedule.
- D. Separate employees into teams led by a person who acts as a single point of contact for observation purposes.

Answer: C

Explanation:

A policy that states employees should use their vacation time in a staggered schedule is a way of employing mandatory vacations. A mandatory vacation policy requires all users to take time away from work while others step in and do the work of that employee on vacation. This will afford the CSO the opportunity to see who is using the company assets responsibly and who is abusing it.

QUESTION NO: 226

A software developer is responsible for writing the code on an accounting application. Another software developer is responsible for developing code on a system in human resources. Once a year they have to switch roles for several weeks.

Which of the following practices is being implemented?

- A. Mandatory vacations
- B. Job rotation
- C. Least privilege
- D. Separation of duties

Answer: B

Explanation:

A job rotation policy defines intervals at which employees must rotate through positions.

QUESTION NO: 227

Which of the following types of risk reducing policies also has the added indirect benefit of cross training employees when implemented?

- A. Least privilege
- B. Job rotation
- C. Mandatory vacations
- D. Separation of duties

Answer: B

Explanation:

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person and it does afford the company with the opportunity to place another person in that same job.

QUESTION NO: 228

In order to prevent and detect fraud, which of the following should be implemented?

- A. Job rotation
- B. Risk analysis
- C. Incident management
- D. Employee evaluations

Answer: A

Explanation:

A job rotation policy defines intervals at which employees must rotate through positions. Similar in purpose to mandatory vacations, it helps to ensure that the company does not become too dependent on one person and it does afford the company with the opportunity to place another person in that same job and in this way the company can potentially uncover any fraud perhaps committed by the incumbent.

QUESTION NO: 229

The Chief Technical Officer (CTO) has been informed of a potential fraud committed by a database administrator performing several other job functions within the company. Which of the following is the BEST method to prevent such activities in the future?

- A. Job rotation
- B. Separation of duties
- C. Mandatory Vacations
- D. Least Privilege

Answer: B

Explanation:

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that you are employing best practices. The segregation of duties and separation of environments is a way to reduce the likelihood of misuse of systems or information. A separation of duties policy is designed to reduce the risk of fraud and to prevent other losses in an organization.

QUESTION NO: 230

Separation of duties is often implemented between developers and administrators in order to separate which of the following?

- A. More experienced employees from less experienced employees
- B. Changes to program code and the ability to deploy to production
- C. Upper level management users from standard development employees
- D. The network access layer from the application access layer

Answer: B

Explanation:

Separation of duties means that there is differentiation between users, employees and duties per se which form part of best practices.

QUESTION NO: 231

A user in the company is in charge of various financial roles but needs to prepare for an upcoming audit. They use the same account to access each financial system. Which of the following security controls will MOST likely be implemented within the company?

- A. Account lockout policy
- B. Account password enforcement

- C. Password complexity enabled
- D. Separation of duties

Answer: D

Explanation:

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that there is differentiation between users, employees and duties per se which form part of best practices.

QUESTION NO: 232

Everyone in the accounting department has the ability to print and sign checks. Internal audit has asked that only one group of employees may print checks while only two other employees may sign the checks. Which of the following concepts would enforce this process?

- A. Separation of Duties
- B. Mandatory Vacations
- C. Discretionary Access Control
- D. Job Rotation

Answer: A

Explanation:

Separation of duties means that users are granted only the permissions they need to do their work and no more.

QUESTION NO: 233

One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

- A. Mandatory access
- B. Rule-based access control
- C. Least privilege
- D. Job rotation

Answer: C

Explanation:

A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

QUESTION NO: 234

A security administrator notices that a specific network administrator is making unauthorized changes to the firewall every Saturday morning. Which of the following would be used to mitigate this issue so that only security administrators can make changes to the firewall?

- A. Mandatory vacations
- B. Job rotation
- C. Least privilege
- D. Time of day restrictions

Answer: C

Explanation:

A least privilege policy is to give users only the permissions that they need to do their work and no more. That is only allowing security administrators to be able to make changes to the firewall by practicing the least privilege principle.

QUESTION NO: 235

Which of the following risk mitigation strategies will allow Ann, a security analyst, to enforce least privilege principles?

- A. User rights reviews
- B. Incident management
- C. Risk based controls
- D. Annual loss expectancy

Answer: A

Explanation:

A least privilege policy should be used when assigning permissions. Give users only the permissions and rights that they need to do their work and no more.

QUESTION NO: 236

An IT security manager is asked to provide the total risk to the business. Which of the following

calculations would the security manager choose to determine total risk?

- A. (Threats X vulnerability X asset value) x controls gap
- B. (Threats X vulnerability X profit) x asset value
- C. Threats X vulnerability X control gap
- D. Threats X vulnerability X asset value

Answer: D

Explanation:

Threats X vulnerability X asset value is equal to asset value (AV) times exposure factor (EF). This is used to calculate a risk.

QUESTION NO: 237

A company is preparing to decommission an offline, non-networked root certificate server. Before sending the server's drives to be destroyed by a contracted company, the Chief Security Officer (CSO) wants to be certain that the data will not be accessed. Which of the following, if implemented, would BEST reassure the CSO? (Select TWO).

- A. Disk hashing procedures
- B. Full disk encryption
- C. Data retention policies
- D. Disk wiping procedures
- E. Removable media encryption

Answer: B,D

Explanation:

B: Full disk encryption is when the entire volume is encrypted; the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption.

D: Disk wiping is the process of overwriting data on the repeatedly, or using a magnet to alter the magnetic structure of the disks. This renders the data unreadable.

QUESTION NO: 238

Identifying residual risk is MOST important to which of the following concepts?

- A. Risk deterrence
- B. Risk acceptance
- C. Risk mitigation

D. Risk avoidance**Answer: B****Explanation:**

Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices exceeds the value of the harm that would occur if the risk came to fruition. To truly qualify as acceptance, it cannot be a risk where the administrator or manager is unaware of its existence; it has to be an identified risk for which those involved understand the potential cost or damage and agree to accept it. Residual risk is always present and will remain a risk thus it should be accepted (risk acceptance)

QUESTION NO: 239

A software company has completed a security assessment. The assessment states that the company should implement fencing and lighting around the property. Additionally, the assessment states that production releases of their software should be digitally signed. Given the recommendations, the company was deficient in which of the following core security areas? (Select TWO).

- A. Fault tolerance
- B. Encryption
- C. Availability
- D. Integrity
- E. Safety
- F. Confidentiality

Answer: D,E**Explanation:**

Aspects such as fencing, proper lighting, locks, CCTV, Escape plans Drills, escape routes and testing controls form part of safety controls.



Integrity refers to aspects such as hashing, digital signatures, certificates and non-repudiation – all of which has to do with data integrity.

QUESTION NO: 240 DRAG DROP



A Security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and Drop the applicable controls to each asset type.

Instructions: Controls can be used multiple times and not all placeholders needs to be filled. When



you have completed the simulation, Please select Done to submit.

Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up Blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mentor app		

Answer:

Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking		
Pop-up Blocker		
Cable Locks		
Antivirus		
Host Based Firewall		
Proximity Reader		
Sniffer		
Mentor app		

Explanation:

Controls	Company Manager Smart Phone	Data Center Terminal Server
Screen Locks		
Strong Password		
Device Encryption		
Remote Wipe		
GPS Tracking	Screen Locks	Cable Locks
Pop-up Blocker	Strong Password	Antivirus
Cable Locks	Device Encryption	Host Based Firewall
Antivirus	Remote Wipe	Proximity Reader
Host Based Firewall	GPS Tracking	Sniffer
Proximity Reader	Pop-up Blocker	Mentor app
Sniffer		
Mentor app		

Cable locks are used as a hardware lock mechanism – thus best used on a Data Center Terminal Server.

Network monitors are also known as sniffers – thus best used on a Data Center Terminal Server. Install antivirus software. Antivirus software should be installed and definitions kept current on all hosts. Antivirus software should run on the server as well as on every workstation. In addition to active monitoring of incoming files, scans should be conducted regularly to catch any infections that have slipped through- thus best used on a Data Center Terminal Server.

Proximity readers are used as part of physical barriers which makes it more appropriate to use on a center's entrance to protect the terminal server.

Mentor app is an Apple application used for personal development and is best used on a mobile device such as a smart phone.

Remote wipe is an application that can be used on devices that are stolen to keep data safe. It is basically a command to a phone that will remotely clear the data on that phone. This process is known as a remote wipe, and it is intended to be used if the phone is stolen or going to another user.

Should a device be stolen, GPS (Global Positioning System) tracking can be used to identify its location and allow authorities to find it - thus best used on a smart phone.

Screen Lock is where the display should be configured to time out after a short period of inactivity and the screen locked with a password. To be able to access the system again, the user must provide the password. After a certain number of attempts, the user should not be allowed to attempt any additional logons; this is called lockout – thus best used on a smart phone.

Strong Password since passwords are always important, but even more so when you consider that the device could be stolen and in the possession of someone who has unlimited access and time to try various values – thus best use strong passwords on a smartphone as it can be stolen more easily than a terminal server in a data center.

Device Encryption- Data should be encrypted on the device so that if it does fall into the wrong

hands, it cannot be accessed in a usable form without the correct passwords. It is recommended to you use Trusted Platform Module (TPM) for all mobile devices where possible.

Use pop-up blockers. Not only are pop-ups irritating, but they are also a security threat. Pop-ups (including pop-underers) represent unwanted programs running on the system, and they can jeopardize the system's well-being. This will be more effective on a mobile device rather than a terminal server.

Use host-based firewalls. A firewall is the first line of defense against attackers and malware. Almost every current operating system includes a firewall, and most are turned on by Default- thus best used on a Data Center Terminal Server.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 221, 222, 369, 418
<http://www.mentor-app.com/>

QUESTION NO: 241

Which of the following defines a business goal for system restoration and acceptable data loss?

- A. MTTR
- B. MTBF
- C. RPO
- D. Warm site

Answer: C

Explanation:

The recovery point objective (RPO) defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). This is an essential business goal insofar as system restoration and acceptable data loss is concerned.

QUESTION NO: 242

Sara, the Chief Security Officer (CSO), has had four security breaches during the past two years.

Each breach has cost the company \$3,000. A third party vendor has offered to repair the security hole in the system for \$25,000. The breached system is scheduled to be replaced in five years.

Which of the following should Sara do to address the risk?

- A. Accept the risk saving \$10,000.
- B. Ignore the risk saving \$5,000.
- C. Mitigate the risk saving \$10,000.
- D. Transfer the risk saving \$5,000.

Answer: D

Explanation:

Risk transference involves sharing some of the risk burden with someone else, such as an insurance company. The cost of the security breach over a period of 5 years would amount to \$30,000 and it is better to save \$5,000.

QUESTION NO: 243

Which of the following concepts are included on the three sides of the "security triangle"? (Select THREE).

- A. Confidentiality
- B. Availability
- C. Integrity
- D. Authorization
- E. Authentication
- F. Continuity

Answer: A,B,C

Explanation:

Confidentiality, integrity, and availability are the three most important concepts in security. Thus they form the security triangle.

QUESTION NO: 244

Elastic cloud computing environments often reuse the same physical hardware for multiple customers over time as virtual machines are instantiated and deleted. This has important implications for which of the following data security concerns?

- A. Hardware integrity
- B. Data confidentiality
- C. Availability of servers
- D. Integrity of data

Answer: B

Explanation:

Data that is not kept separate or segregated will impact on that data's confidentiality maybe being compromised. Be aware of the fact that your data is only as safe as the data with which it is integrated. For example, assume that your client database is hosted on a server that another company is also using to test an application that they are creating. If their application obtains root-level access at some point (such as to change passwords) and crashes at that point, then the user running the application could be left with root permissions and conceivably be to access data on the server for which they are not authorized, such as your client database. Data segregation is crucial; keep your data on secure servers.

QUESTION NO: 245

The system administrator notices that their application is no longer able to keep up with the large amounts of traffic their server is receiving daily. Several packets are dropped and sometimes the server is taken offline. Which of the following would be a possible solution to look into to ensure their application remains secure and available?

- A. Cloud computing
- B. Full disk encryption
- C. Data Loss Prevention
- D. HSM

Answer: A

Explanation:

Cloud computing means hosting services and data on the Internet instead of hosting it locally. There is thus no issue when the company's server is taken offline.

QUESTION NO: 246

Users can authenticate to a company's web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?

- A. Malicious users can exploit local corporate credentials with their social media credentials
- B. Changes to passwords on the social media site can be delayed from replicating to the company
- C. Data loss from the corporate servers can create legal liabilities with the social media site
- D. Password breaches to the social media site affect the company application as well

Answer: D

Explanation:

Social networking and having your company's application authentication 'linked' to users' credentials that they use on social media sites exposes your company's application exponentially more than is necessary. You should strive to practice risk avoidance.

QUESTION NO: 247

Which of the following is the GREATEST security risk of two or more companies working together under a Memorandum of Understanding?

- A.** Budgetary considerations may not have been written into the MOU, leaving an entity to absorb more cost than intended at signing.
- B.** MOUs have strict policies in place for services performed between the entities and the penalties for compromising a partner are high.
- C.** MOUs are generally loose agreements and therefore may not have strict guidelines in place to protect sensitive data between the two entities.
- D.** MOUs between two companies working together cannot be held to the same legal standards as SLAs.

Answer: C

Explanation:

The Memorandum of Understanding This document is used in many settings in the information industry. It is a brief summary of which party is responsible for what portion of the work. For example, Company A may be responsible for maintaining the database server and Company B may be responsible for telecommunications. MOUs are not legally binding but they carry a degree of seriousness and mutual respect, stronger than a gentlemen's agreement. Often, MOUs are the first steps towards a legal contract.

QUESTION NO: 248

Which of the following describes the purpose of an MOU?

- A.** Define interoperability requirements
- B.** Define data backup process
- C.** Define onboard/offboard procedure
- D.** Define responsibilities of each party

Answer: D

Explanation:

MOU or Memorandum of Understanding is a document outlining which party is responsible for what portion of the work.

QUESTION NO: 249

A company has decided to move large data sets to a cloud provider in order to limit the costs of new infrastructure. Some of the data is sensitive and the Chief Information Officer wants to make sure both parties have a clear understanding of the controls needed to protect the data.

Which of the following types of interoperability agreement is this?

- A. ISA
- B. MOU
- C. SLA
- D. BPA

Answer: A

Explanation:

ISA/ Interconnection Security Agreement is an agreement between two organizations that have connected systems. The agreement documents the technical requirements of the connected systems.

QUESTION NO: 250

Which of the following is the primary security concern when deploying a mobile device on a network?

- A. Strong authentication
- B. Interoperability
- C. Data security
- D. Cloud storage technique

Answer: C

Explanation:

Mobile devices, such as laptops, tablet computers, and smartphones, provide security challenges above those of desktop workstations, servers, and such in that they leave the office and this increases the odds of their theft which makes data security a real concern. At a bare minimum, the following security measures should be in place on mobile devices: Screen lock, Strong password, Device encryption, Remote Wipe or Sanitation, voice encryption, GPS tracking, Application

control, storage segmentation, asset tracking and device access control.

QUESTION NO: 251

A security administrator plans on replacing a critical business application in five years. Recently, there was a security flaw discovered in the application that will cause the IT department to manually re-enable user accounts each month at a cost of \$2,000. Patching the application today would cost \$140,000 and take two months to implement. Which of the following should the security administrator do in regards to the application?

- A. Avoid the risk to the user base allowing them to re-enable their own accounts
- B. Mitigate the risk by patching the application to increase security and saving money
- C. Transfer the risk replacing the application now instead of in five years
- D. Accept the risk and continue to enable the accounts each month saving money

Answer: D

Explanation:

This is a risk acceptance measure that has to be implemented since the cost of patching would be too high compared to the cost to keep the system going as is. Risk acceptance is often the choice you must make when the cost of implementing any of the other four choices (i.e. risk deterrence, mitigation, transference or avoidance) exceeds the value of the harm that would occur if the risk came to fruition.

QUESTION NO: 252

Acme Corp has selectively outsourced proprietary business processes to ABC Services. Due to some technical issues, ABC services wants to send some of Acme Corp's debug data to a third party vendor for problem resolution. Which of the following **MUST** be considered prior to sending data to a third party?

- A. The data should be encrypted prior to transport
- B. This would not constitute unauthorized data sharing
- C. This may violate data ownership and non-disclosure agreements
- D. Acme Corp should send the data to ABC Services' vendor instead

Answer: C

Explanation:

With sending your data to a third party is already a risk since the third party may have a different policy than yours. Data ownership and non-disclosure is already a risk that you will have to accept since the data will be sent for debugging /troubleshooting purposes which will result in definite

disclosure of the data.

QUESTION NO: 253

An administrator wants to minimize the amount of time needed to perform backups during the week. It is also acceptable to the administrator for restoration to take an extended time frame.

Which of the following strategies would the administrator MOST likely implement?

- A. Full backups on the weekend and incremental during the week
- B. Full backups on the weekend and full backups every day
- C. Incremental backups on the weekend and differential backups every day
- D. Differential backups on the weekend and full backups every day

Answer: A

Explanation:

A full backup is a complete, comprehensive backup of all files on a disk or server. The full backup is current only at the time it's performed. Once a full backup is made, you have a complete archive of the system at that point in time. A system shouldn't be in use while it undergoes a full backup because some files may not get backed up. Once the system goes back into operation, the backup is no longer current. A full backup can be a time-consuming process on a large system. An incremental backup is a partial backup that stores only the information that has been changed since the last full or the last incremental backup. If a full backup were performed on a Sunday night, an incremental backup done on Monday night would contain only the information that changed since Sunday night. Such a backup is typically considerably smaller than a full backup. Each incremental backup must be retained until a full backup can be performed. Incremental backups are usually the fastest backups to perform on most systems, and each incremental backup tape is relatively small.

QUESTION NO: 254

A security administrator needs to update the OS on all the switches in the company. Which of the following MUST be done before any actual switch configuration is performed?

- A. The request needs to be sent to the incident management team.
- B. The request needs to be approved through the incident management process.
- C. The request needs to be approved through the change management process.
- D. The request needs to be sent to the change management team.

Answer: C

Explanation:

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. Thus the actual switch configuration should first be subject to the change management approval.

QUESTION NO: 255

Developers currently have access to update production servers without going through an approval process. Which of the following strategies would BEST mitigate this risk?

- A. Incident management
- B. Clean desk policy
- C. Routine audits
- D. Change management

Answer: D

Explanation:

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. This structured approach involves policies that should be in place and technological controls that should be enforced.

QUESTION NO: 256

Which of the following mitigation strategies is established to reduce risk when performing updates to business critical systems?

- A. Incident management
- B. Server clustering
- C. Change management
- D. Forensic analysis

Answer: C

Explanation:

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case 'performing updates to business critical systems.

QUESTION NO: 257

The network administrator is responsible for promoting code to applications on a DMZ web server. Which of the following processes is being followed to ensure application integrity?

- A. Application hardening
- B. Application firewall review
- C. Application change management
- D. Application patch management

Answer: C

Explanation:

Change management is the structured approach that is followed to secure a company's assets. Promoting code to application on a SMZ web server would be change management.

QUESTION NO: 258

Which of the following MOST specifically defines the procedures to follow when scheduled system patching fails resulting in system outages?

- A. Risk transference
- B. Change management
- C. Configuration management
- D. Access control revalidation

Answer: B

Explanation:

Change Management is a risk mitigation approach and refers to the structured approach that is followed to secure a company's assets. In this case 'scheduled system patching'.

QUESTION NO: 259

A security engineer is given new application extensions each month that need to be secured prior to implementation. They do not want the new extensions to invalidate or interfere with existing application security. Additionally, the engineer wants to ensure that the new requirements are approved by the appropriate personnel. Which of the following should be in place to meet these two goals? (Select TWO).

- A. Patch Audit Policy
- B. Change Control Policy

- C. Incident Management Policy
- D. Regression Testing Policy
- E. Escalation Policy
- F. Application Audit Policy

Answer: B,D

Explanation:

A backout (regression testing) is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout. A change control policy refers to the structured approach that is followed to secure a company's assets in the event of changes occurring.

QUESTION NO: 260

A user has received an email from an external source which asks for details on the company's new product line set for release in one month. The user has a detailed spec sheet but it is marked "Internal Proprietary Information". Which of the following should the user do NEXT?

- A. Contact their manager and request guidance on how to best move forward
- B. Contact the help desk and/or incident response team to determine next steps
- C. Provide the requestor with the email information since it will be released soon anyway
- D. Reply back to the requestor to gain their contact information and call them

Answer: B

Explanation:

This is an incident that has to be responded to by the person who discovered it- in this case the user. An incident is any attempt to violate a security policy, a successful penetration, a compromise of a system, or any unauthorized access to information. It's important that an incident response policy establish at least the following items:

Outside agencies that should be contacted or notified in case of an incident

Resources used to deal with an incident

Procedures to gather and secure evidence

List of information that should be collected about an incident

Outside experts who can be used to address issues if needed

Policies and guidelines regarding how to handle an incident

Since the spec sheet has been marked Internal Proprietary Information the user should refer the incident to the incident response team.

QUESTION NO: 261

Which of the following is BEST carried out immediately after a security breach is discovered?

- A. Risk transference
- B. Access control revalidation
- C. Change management
- D. Incident management

Answer: D

Explanation:

Incident management is the steps followed when security incident occurs.

QUESTION NO: 262

A security analyst informs the Chief Executive Officer (CEO) that a security breach has just occurred. This results in the Risk Manager and Chief Information Officer (CIO) being caught unaware when the CEO asks for further information. Which of the following strategies should be implemented to ensure the Risk Manager and CIO are not caught unaware in the future?

- A. Procedure and policy management
- B. Chain of custody management
- C. Change management
- D. Incident management

Answer: D

Explanation:

incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets). The events that could occur include security breaches.

QUESTION NO: 263

Requiring technicians to report spyware infections is a step in which of the following?

- A. Routine audits
- B. Change management
- C. Incident management
- D. Clean desk policy

Answer: C

Explanation:

Incident management refers to the steps followed when events occur (making sure controls are in place to prevent unauthorized access to, and changes of, all IT assets).

QUESTION NO: 264

Which of the following is the BEST approach to perform risk mitigation of user access control rights?

- A. Conduct surveys and rank the results.
- B. Perform routine user permission reviews.
- C. Implement periodic vulnerability scanning.
- D. Disable user accounts that have not been used within the last two weeks.

Answer: B

Explanation:

Risk mitigation is accomplished any time you take steps to reduce risk. This category includes installing antivirus software, educating users about possible threats, monitoring network traffic, adding a firewall, and so on. User permissions may be the most basic aspect of security and is best coupled with a principle of least privilege. And related to permissions is the concept of the access control list (ACL). An ACL is literally a list of who can access what resource and at what level. Thus the best risk mitigation steps insofar as access control rights are concerned, is the regular/routine review of user permissions.

QUESTION NO: 265

An internal auditor is concerned with privilege creep that is associated with transfers inside the company. Which mitigation measure would detect and correct this?

- A. User rights reviews
- B. Least privilege and job rotation
- C. Change management
- D. Change Control

Answer: A

Explanation:

A privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of an organization. This means that a user rights review will reveal whether user accounts have been assigned according to their 'new' job descriptions, or if there are privilege creep culprits after transfers has occurred.

QUESTION NO: 266

A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

- A.** Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.
- B.** Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.
- C.** Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.
- D.** Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Answer: A

Explanation:

Reviewing user permissions and group memberships form part of a privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation.

QUESTION NO: 267

Various network outages have occurred recently due to unapproved changes to network and security devices. All changes were made using various system credentials. The security analyst has been tasked to update the security policy. Which of the following risk mitigation strategies would also need to be implemented to reduce the number of network outages due to unauthorized changes?

- A.** User rights and permissions review
- B.** Configuration management
- C.** Incident management
- D.** Implement security controls on Layer 3 devices

Answer: A

Explanation:

Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions. Also reviewing user rights and permissions will afford the security analyst the opportunity to put the principle of least privilege in practice as well as update the security policy

QUESTION NO: 268

After an audit, it was discovered that the security group memberships were not properly adjusted for employees' accounts when they moved from one role to another. Which of the following has the organization failed to properly implement? (Select TWO).

- A. Mandatory access control enforcement.
- B. User rights and permission reviews.
- C. Technical controls over account management.
- D. Account termination procedures.
- E. Management controls over account management.
- F. Incident management and response plan.

Answer: B,E

Explanation:

Reviewing user rights and permissions can be used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation and their job descriptions since they were all moved to different roles.

Control over account management would have taken into account the different roles that employees have and adjusted the rights and permissions of these roles accordingly.

QUESTION NO: 269

The security administrator is currently unaware of an incident that occurred a week ago. Which of the following will ensure the administrator is notified in a timely manner in the future?

- A. User permissions reviews
- B. Incident response team
- C. Change management
- D. Routine auditing

Answer: D

Explanation:

Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.

QUESTION NO: 270

The system administrator has deployed updated security controls for the network to limit risk of attack. The security manager is concerned that controls continue to function as intended to maintain appropriate security posture.

Which of the following risk mitigation strategies is MOST important to the security manager?

- A. User permissions
- B. Policy enforcement
- C. Routine audits
- D. Change management

Answer: C

Explanation:

After you have implemented security controls based on risk, you must perform routine audits. These audits should include reviews of user rights and permissions as well as specific events. You should pay particular attention to false positives and negatives.

QUESTION NO: 271

Which of the following security account management techniques should a security analyst implement to prevent staff, who has switched company roles, from exceeding privileges?

- A. Internal account audits
- B. Account disablement
- C. Time of day restriction
- D. Password complexity

Answer: A

Explanation:

Internal account auditing will allow you to switch the appropriate users to the proper accounts required after the switching of roles occurred and thus check that the principle of least privilege is followed.

QUESTION NO: 272

Encryption of data at rest is important for sensitive information because of which of the following?

- A. Facilitates tier 2 support, by preventing users from changing the OS
- B. Renders the recovery of data harder in the event of user password loss
- C. Allows the remote removal of data following eDiscovery requests
- D. Prevents data from being accessed following theft of physical equipment

Answer: D

Explanation:

Data encryption allows data that has been stolen to remain out of the eyes of the intruders who took it as long as they do not have the proper passwords.

QUESTION NO: 273

A company is trying to limit the risk associated with the use of unapproved USB devices to copy documents. Which of the following would be the BEST technology control to use in this scenario?

- A. Content filtering
- B. IDS
- C. Audit logs
- D. DLP

Answer: D

Explanation:

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

QUESTION NO: 274

Several employees have been printing files that include personally identifiable information of customers. Auditors have raised concerns about the destruction of these hard copies after they are created, and management has decided the best way to address this concern is by preventing these files from being printed.

Which of the following would be the BEST control to implement?

- A. File encryption
- B. Printer hardening
- C. Clean desk policies
- D. Data loss prevention

Answer: D

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. This would address the concerns of the auditors.

QUESTION NO: 275

Which of the following security strategies allows a company to limit damage to internal systems and provides loss control?

- A. Restoration and recovery strategies
- B. Deterrent strategies
- C. Containment strategies
- D. Detection strategies

Answer: C

Explanation:

Containment strategies is used to limit damages, contain a loss so that it may be controlled, much like quarantine, and loss incident isolation.

QUESTION NO: 276

Matt, a security analyst, needs to implement encryption for company data and also prevent theft of company data. Where and how should Matt meet this requirement?

- A. Matt should implement access control lists and turn on EFS.
- B. Matt should implement DLP and encrypt the company database.
- C. Matt should install Truecrypt and encrypt the company server.
- D. Matt should install TPMs and encrypt the company database.

Answer: B

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and

networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Encryption is used to protect data.

QUESTION NO: 277

An employee recently lost a USB drive containing confidential customer data. Which of the following controls could be utilized to minimize the risk involved with the use of USB drives?

- A. DLP
- B. Asset tracking
- C. HSM
- D. Access control

Answer: A

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

QUESTION NO: 278

Which of the following controls would prevent an employee from emailing unencrypted information to their personal email account over the corporate network?

- A. DLP
- B. CRL
- C. TPM
- D. HSM

Answer: A

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data.

QUESTION NO: 279

Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

- A. Scanning printing of documents.
- B. Scanning of outbound IM (Instance Messaging).
- C. Scanning copying of documents to USB.
- D. Scanning of SharePoint document library.
- E. Scanning of shared drives.
- F. Scanning of HTTP user traffic.

Answer: B,F

Explanation:

DLP systems monitor the contents of systems (workstations, servers, networks) to make sure key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Outbound IM and HTTP user traffic refers to data over a network which falls within the DLP strategy.

QUESTION NO: 280

Which of the following assets is MOST likely considered for DLP?

- A. Application server content
- B. USB mass storage devices
- C. Reverse proxy
- D. Print server

Answer: B

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. A USB presents the most likely device to be used to steal data because of its physical size.

QUESTION NO: 281

The Chief Information Officer (CIO) is concerned with moving an application to a SaaS cloud provider. Which of the following can be implemented to provide for data confidentiality assurance during and after the migration to the cloud?

- A. HPM technology
- B. Full disk encryption
- C. DLP policy
- D. TPM technology

Answer: C

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. The Software as a Service (SaaS) applications are remotely run over the Web and as such requires DLP monitoring.

QUESTION NO: 282

Which of the following is a Data Loss Prevention (DLP) strategy and is MOST useful for securing data in use?

- A. Email scanning
- B. Content discovery
- C. Database fingerprinting
- D. Endpoint protection

Answer: D

Explanation:

Data loss prevention (DLP) systems monitor the contents of systems (workstations, servers, and networks) to make sure that key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. DLP systems share commonality with network intrusion prevention systems. Endpoint protection provides security and management over both physical and virtual environments.

QUESTION NO: 283

A customer service department has a business need to send high volumes of confidential information to customers electronically. All emails go through a DLP scanner. Which of the following is the BEST solution to meet the business needs and protect confidential information?

- A. Automatically encrypt impacted outgoing emails
- B. Automatically encrypt impacted incoming emails
- C. Monitor impacted outgoing emails
- D. Prevent impacted outgoing emails

Answer: A

Explanation:

Encryption is done to protect confidentiality and integrity of data. It also provides authentication, nonrepudiation and access control to the data. Since all emails go through a DLP scanner and it is outgoing mail that requires protection then the best option is to put a system in place that will encrypt the outgoing emails automatically.

QUESTION NO: 284

Which of the following is a best practice when a mistake is made during a forensics examination?

- A. The examiner should verify the tools before, during, and after an examination.
- B. The examiner should attempt to hide the mistake during cross-examination.
- C. The examiner should document the mistake and workaround the problem.
- D. The examiner should disclose the mistake and assess another area of the disc.

Answer: C

Explanation:

Every step in an incident response should be documented, including every action taken by end users and the incident-response team.

QUESTION NO: 285

An incident response team member needs to perform a forensics examination but does not have the required hardware. Which of the following will allow the team member to perform the examination with minimal impact to the potential evidence?

- A. Using a software file recovery disc
- B. Mounting the drive in read-only mode
- C. Imaging based on order of volatility
- D. Hashing the image after capture

Answer: B

Explanation:

Mounting the drive in read-only mode will prevent any executable commands from being executed. This in turn will have the least impact on potential evidence using the drive in question.

QUESTION NO: 286 DRAG DROP

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

1

2

3

4

RAM

CPU cache

Swap

Hard drive

Answer:

1 CPU cache

2 RAM

3 Swap

4 Hard drive

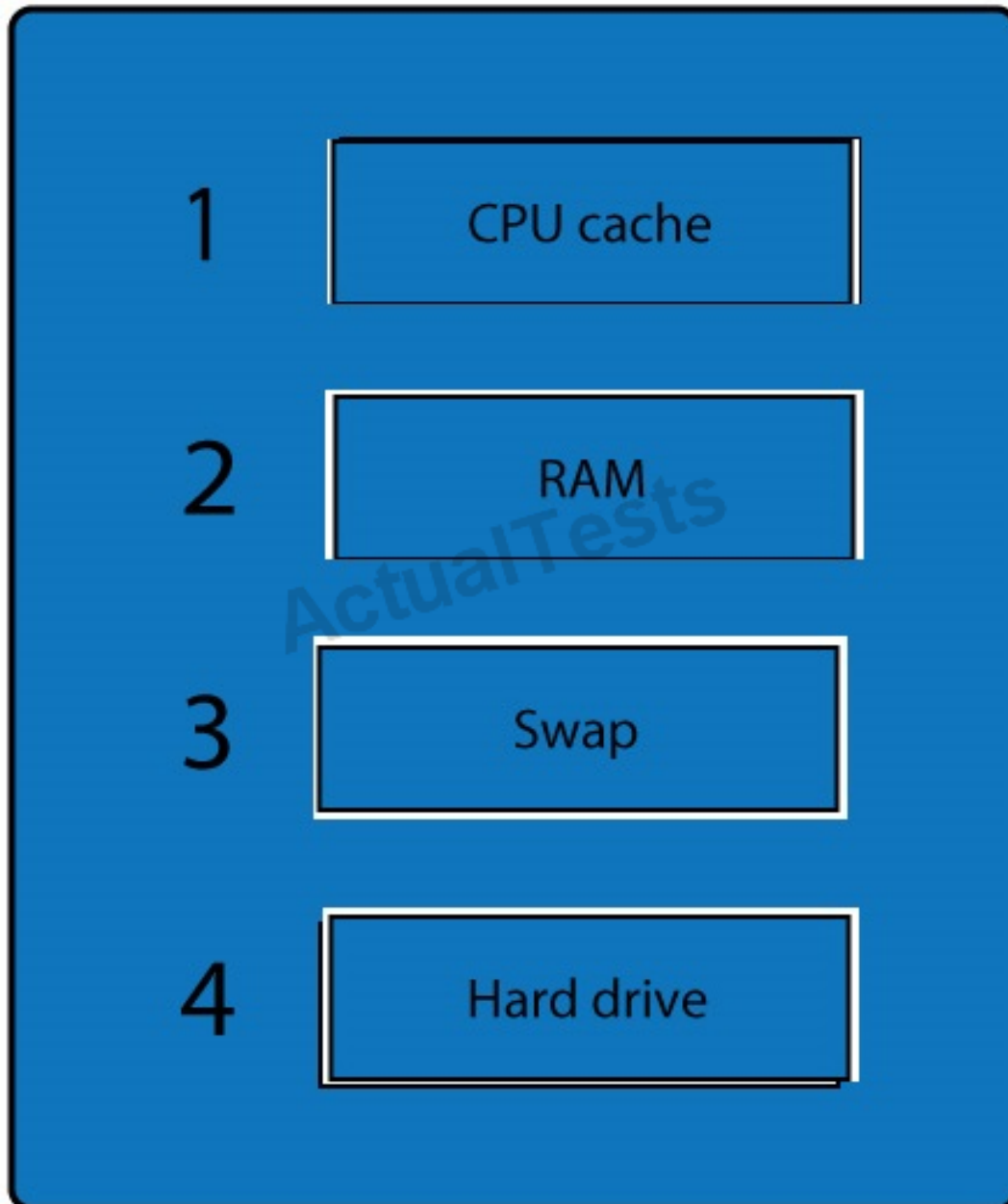
RAM

CPU cache

Swap

Hard drive

Explanation:



When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex,

Indianapolis, 2014, p. 453

QUESTION NO: 287

Which of the following should Jane, a security administrator, perform before a hard drive is analyzed with forensics tools?

- A. Identify user habits
- B. Disconnect system from network
- C. Capture system image
- D. Interview witnesses

Answer: C

Explanation:

Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. Very much as helpful in same way that a virus sample is kept in laboratories to study later after a breakout. Also you should act in the order of volatility which states that the system image capture is first on the list of a forensic analysis.

QUESTION NO: 288

Computer evidence at a crime is preserved by making an exact copy of the hard disk. Which of the following does this illustrate?

- A. Taking screenshots
- B. System image capture
- C. Chain of custody
- D. Order of volatility

Answer: B

Explanation:

A system image would be a snapshot of what exists at the moment. Thus capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

QUESTION NO: 289

To ensure proper evidence collection, which of the following steps should be performed FIRST?

- A. Take hashes from the live system
- B. Review logs
- C. Capture the system image
- D. Copy all compromised files

Answer: C

Explanation:

Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it. This is essential since the collection of evidence process may result in some mishandling and changing the exploited state.

QUESTION NO: 290

A security administrator needs to image a large hard drive for forensic analysis. Which of the following will allow for faster imaging to a second hard drive?

- A. `cp /dev/sda /dev/sdb bs=8k`
- B. `tail -f /dev/sda > /dev/sdb bs=8k`
- C. `dd in=/dev/sda out=/dev/sdb bs=4k`
- D. `locate /dev/sda /dev/sdb bs=4k`

Answer: C

Explanation:

dd is a command-line utility for Unix and Unix-like operating systems whose primary purpose is to convert and copy files. dd can duplicate data across files, devices, partitions and volumes. On Unix, device drivers for hardware (such as hard disks) and special device files (such as `/dev/zero` and `/dev/random`) appear in the file system just like normal files; dd can also read and/or write from/to these files, provided that function is implemented in their respective driver. As a result, dd can be used for tasks such as backing up the boot sector of a hard drive, and obtaining a fixed amount of random data. The dd program can also perform conversions on the data as it is copied, including byte order swapping and conversion to and from the ASCII and EBCDIC text encodings.

An attempt to copy the entire disk using cp may omit the final block if it is of an unexpected length; whereas dd may succeed. The source and destination disks should have the same size.

QUESTION NO: 291

A security technician wishes to gather and analyze all Web traffic during a particular time period.

Which of the following represents the BEST approach to gathering the required data?

- A. Configure a VPN concentrator to log all traffic destined for ports 80 and 443.
- B. Configure a proxy server to log all traffic destined for ports 80 and 443.
- C. Configure a switch to log all traffic destined for ports 80 and 443.
- D. Configure a NIDS to log all traffic destined for ports 80 and 443.

Answer: B

Explanation:

A proxy server is in essence a device that acts on behalf of others and in security terms all internal user interaction with the Internet should be controlled through a proxy server. This makes a proxy server the best tool to gather the required data.

QUESTION NO: 292

A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site were facing the wrong direction to capture the incident. The analyst ensures the cameras are turned to face the proper direction. Which of the following types of controls is being used?

- A. Detective
- B. Deterrent
- C. Corrective
- D. Preventive

Answer: C

Explanation:

A corrective control would be any corrective action taken to correct any existing control that were faulty or wrongly installed – as in this case the cameras were already there, it just had to be adjusted to perform its function as intended.

QUESTION NO: 293

Joe, a security administrator, is concerned with users tailgating into the restricted areas. Given a limited budget, which of the following would BEST assist Joe with detecting this activity?

- A. Place a full-time guard at the entrance to confirm user identity.
- B. Install a camera and DVR at the entrance to monitor access.

- C. Revoke all proximity badge access to make users justify access.
- D. Install a motion detector near the entrance.

Answer: B

Explanation:

Tailgating is a favorite method of gaining entry to electronically locked systems by following someone through the door they just unlocked. With a limited budget installing a camera and DVR at the entrance to monitor access to the restricted areas is the most feasible solution. The benefit of a camera (also known as closed-circuit television, or CCTV) is that it is always running and can record everything it sees, creating evidence that can be admissible in court if necessary.

QUESTION NO: 294

The incident response team has received the following email message.

From: monitor@ext-company.com

To: security@company.com

Subject: Copyright infringement

A copyright infringement alert was triggered by IP address 13.10.66.5 at 09: 50: 01 GMT.

After reviewing the following web logs for IP 13.10.66.5, the team is unable to correlate and identify the incident.

09: 45: 33 13.10.66.5 http: //remote.site.com/login.asp?user=john

09: 50: 22 13.10.66.5 http: //remote.site.com/logout.asp?user=anne

10: 50: 01 13.10.66.5 http: //remote.site.com/access.asp?file=movie.mov

11: 02: 45 13.10.65.5 http: //remote.site.com/download.asp?movie.mov=ok

Which of the following is the MOST likely reason why the incident response team is unable to identify and correlate the incident?

- A. The logs are corrupt and no longer forensically sound.
- B. Traffic logs for the incident are unavailable.
- C. Chain of custody was not properly maintained.
- D. Incident time offsets were not accounted for.

Answer: D

Explanation:

It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system.

QUESTION NO: 295

A system administrator is responding to a legal order to turn over all logs from all company servers. The system administrator records the system time of all servers to ensure that:

- A. HDD hashes are accurate.
- B. the NTP server works properly.
- C. chain of custody is preserved.
- D. time offset can be calculated.

Answer: D**Explanation:**

It is quite common for workstation times to be off slightly from actual time, and that can happen with servers as well. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system.

QUESTION NO: 296

A recent intrusion has resulted in the need to perform incident response procedures. The incident response team has identified audit logs throughout the network and organizational systems which hold details of the security breach. Prior to this incident, a security consultant informed the company that they needed to implement an NTP server on the network. Which of the following is a problem that the incident response team will likely encounter during their assessment?

- A. Chain of custody
- B. Tracking man hours
- C. Record time offset
- D. Capture video traffic

Answer: C

Explanation:

It is quite common for workstation as well as server times to be off slightly from actual time. Since a forensic investigation is usually dependent on a step-by-step account of what has happened, being able to follow events in the correct time sequence is critical. Because of this, it is imperative to record the time offset on each affected machine during the investigation. One method of assisting with this is to add an entry to a log file and note the time that this was done and the time associated with it on the system. There is no mention that this was done by the incident response team.

QUESTION NO: 297

Computer evidence at a crime scene is documented with a tag stating who had possession of the evidence at a given time.

Which of the following does this illustrate?

- A. System image capture
- B. Record time offset
- C. Order of volatility
- D. Chain of custody

Answer: D

Explanation:

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been.

QUESTION NO: 298

A compromised workstation utilized in a Distributed Denial of Service (DDOS) attack has been removed from the network and an image of the hard drive has been created. However, the system administrator stated that the system was left unattended for several hours before the image was created. In the event of a court case, which of the following is likely to be an issue with this incident?

- A. Eye Witness
- B. Data Analysis of the hard drive
- C. Chain of custody

D. Expert Witness**Answer: C****Explanation:**

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering.

QUESTION NO: 299

The security manager received a report that an employee was involved in illegal activity and has saved data to a workstation's hard drive. During the investigation, local law enforcement's criminal division confiscates the hard drive as evidence. Which of the following forensic procedures is involved?

- A.** Chain of custody
- B.** System image
- C.** Take hashes
- D.** Order of volatility

Answer: A**Explanation:**

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it. When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been.

QUESTION NO: 300

Which of the following is the MOST important step for preserving evidence during forensic procedures?

- A.** Involve law enforcement
- B.** Chain of custody
- C.** Record the time of the incident
- D.** Report within one hour of discovery

Answer: B**Explanation:**

Chain of custody deals with how evidence is secured, where it is stored, and who has access to it.

When you begin to collect evidence, you must keep track of that evidence at all times and show who has it, who has seen it, and where it has been. The evidence must always be within your custody, or you're open to dispute about possible evidence tampering. Thus to preserve evidence during a forensic procedure the chain of custody is of utmost importance.

QUESTION NO: 301

During which of the following phases of the Incident Response process should a security administrator define and implement general defense against malware?

- A. Lessons Learned
- B. Preparation
- C. Eradication
- D. Identification

Answer: B

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. It is important to stop malware before it ever gets hold of a system –thus you should know which malware is out there and take defensive measures - this means preparation to guard against malware infection should be done.

QUESTION NO: 302

The Chief Technical Officer (CTO) has tasked The Computer Emergency Response Team (CERT) to develop and update all Internal Operating Procedures and Standard Operating Procedures documentation in order to successfully respond to future incidents. Which of the following stages of the Incident Handling process is the team working on?

- A. Lessons Learned
- B. Eradication
- C. Recovery
- D. Preparation

Answer: D

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and

notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Developing and updating all internal operating and standard operating procedures documentation to handle future incidents is preparation.

QUESTION NO: 303

The helpdesk reports increased calls from clients reporting spikes in malware infections on their systems. Which of the following phases of incident response is MOST appropriate as a FIRST response?

- A. Recovery
- B. Follow-up
- C. Validation
- D. Identification
- E. Eradication
- F. Containment

Answer: D

Explanation:

To be able to respond to the incident of malware infection you need to know what type of malware was used since there are many types of malware around. This makes identification critical in this case.

QUESTION NO: 304

Who should be contacted FIRST in the event of a security breach?

- A. Forensics analysis team
- B. Internal auditors
- C. Incident response team
- D. Software vendors

Answer: C

Explanation:

A security breach is an incident and requires a response. The incident response team would be better equipped to deal with any incident insofar as all their procedures are concerned. Their procedures in addressing incidents are: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First

responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control.

QUESTION NO: 305

In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence?

- A. Mitigation
- B. Identification
- C. Preparation
- D. Lessons learned

Answer: D

Explanation:

Incident response procedures involves in chronological order: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Thus lessons are only learned after the mitigation occurred. For only then can you 'step back' and analyze the incident to prevent the same occurrence in future.

QUESTION NO: 306

After a recent security breach, the network administrator has been tasked to update and backup all router and switch configurations. The security administrator has been tasked to enforce stricter security policies. All users were forced to undergo additional user awareness training. All of these actions are due to which of the following types of risk mitigation strategies?

- A. Change management
- B. Implementing policies to prevent data loss
- C. User rights and permissions review
- D. Lessons learned

Answer: D

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Described in the question is a situation where a security breach had occurred and its

response which shows that lessons have been learned and used to put in place measures that will prevent any future security breaches of the same kind.

QUESTION NO: 307

A server dedicated to the storage and processing of sensitive information was compromised with a rootkit and sensitive data was extracted. Which of the following incident response procedures is best suited to restore the server?

- A.** Wipe the storage, reinstall the OS from original media and restore the data from the last known good backup.
- B.** Keep the data partition, restore the OS from the most current backup and run a full system antivirus scan.
- C.** Format the storage and reinstall both the OS and the data from the most current backup.
- D.** Erase the storage, reinstall the OS from most current backup and only restore the data that was not compromised.

Answer: A

Explanation:

Rootkits are software programs that have the ability to hide certain things from the operating system. With a rootkit, there may be a number of processes running on a system that do not show up in Task Manager or connections established or available that do not appear in a netstat display—the rootkit masks the presence of these items. The rootkit is able to do this by manipulating function calls to the operating system and filtering out information that would normally appear. Theoretically, rootkits could hide anywhere that there is enough memory to reside: video cards, PCI cards, and the like. The best way to handle this situation is to wipe the server and reinstall the operating system with the original installation disks and then restore the extracted data from your last known good backup. This way you can eradicate the rootkit and restore the data.

QUESTION NO: 308

In the initial stages of an incident response, Matt, the security administrator, was provided the hard drives in question from the incident manager. Which of the following incident response procedures would he need to perform in order to begin the analysis? (Select TWO).

- A.** Take hashes
- B.** Begin the chain of custody paperwork
- C.** Take screen shots

- D. Capture the system image
- E. Decompile suspicious files

Answer: A,D

Explanation:

A: Take Hashes. NIST (the National Institute of Standards and Technology) maintains a National Software Reference Library (NSRL). One of the purposes of the NSRL is to collect “known, traceable software applications” through their hash values and store them in a Reference Data Set (RDS). The RDS can then be used by law enforcement, government agencies, and businesses to determine which files are important as evidence in criminal investigations.

D: A system image is a snapshot of what exists. Capturing an image of the operating system in its exploited state can be helpful in revisiting the issue after the fact to learn more about it.

QUESTION NO: 309

Which of the following is the LEAST volatile when performing incident response procedures?

- A. Registers
- B. RAID cache
- C. RAM
- D. Hard drive

Answer: D

Explanation:

An example of OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts. Of the options stated in the question the hard drive would be the least volatile.

QUESTION NO: 310

The security officer is preparing a read-only USB stick with a document of important personal phone numbers, vendor contacts, an MD5 program, and other tools to provide to employees. At which of the following points in an incident should the officer instruct employees to use this information?

- A. Business Impact Analysis
- B. First Responder
- C. Damage and Loss Control
- D. Contingency Planning

Answer: B

Explanation:

Incident response procedures involves: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. In this scenario the security officer is carrying out an incident response measure that will address and be of benefit to those in the vanguard, i.e. the employees and they are the first responders.

QUESTION NO: 311

After a number of highly publicized and embarrassing customer data leaks as a result of social engineering attacks by phone, the Chief Information Officer (CIO) has decided user training will reduce the risk of another data leak. Which of the following would be MOST effective in reducing data leaks in this situation?

- A. Information Security Awareness
- B. Social Media and BYOD
- C. Data Handling and Disposal
- D. Acceptable Use of IT Systems

Answer: A

Explanation:

Education and training with regard to Information Security Awareness will reduce the risk of data leaks and as such forms an integral part of Security Awareness. By employing social engineering data can be leaked by employees and only when company users are made aware of the methods of social engineering via Information Security Awareness Training, you can reduce the risk of data leaks.

QUESTION NO: 312

Sara, a company's security officer, often receives reports of unauthorized personnel having access codes to the cipher locks of secure areas in the building. Sara should immediately implement which of the following?

- A. Acceptable Use Policy
- B. Physical security controls
- C. Technical controls
- D. Security awareness training

Answer: D

Explanation:

Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. A good security awareness training program for the entire organization should cover the following areas: Importance of security; Responsibilities of people in the organization; Policies and procedures; Usage policies; Account and password-selection criteria as well as Social engineering prevention.

QUESTION NO: 313

Human Resources (HR) would like executives to undergo only two specific security training programs a year. Which of the following provides the BEST level of security training for the executives? (Select TWO).

- A. Acceptable use of social media
- B. Data handling and disposal
- C. Zero day exploits and viruses
- D. Phishing threats and attacks
- E. Clean desk and BYOD
- F. Information security awareness

Answer: D,F

Explanation:

Managers/ i.e. executives in the company are concerned with more global issues in the organization, including enforcing security policies and procedures. Managers should receive additional training or exposure that explains the issues, threats, and methods of dealing with threats. Management will also be concerned about productivity impacts and enforcement and how the various departments are affected by security policies.

Phishing is a form of social engineering in which you ask someone for a piece of information that you are missing by making it look as if it is a legitimate request. An email might look as if it is from a bank and contain some basic information, such as the user's name. Executives are easily fall prey to phishing if they are not trained to lookout for these attacks.

QUESTION NO: 314

The method to provide end users of IT systems and applications with requirements related to acceptable use, privacy, new threats and trends, and use of social networking is:

- A. Security awareness training.
- B. BYOD security training.
- C. Role-based security training.
- D. Legal compliance training.

Answer: A

Explanation:

Security awareness and training are critical to the success of a security effort. They include explaining policies, procedures, and current threats to both users and management.

QUESTION NO: 315

Sara, an employee, tethers her smartphone to her work PC to bypass the corporate web security gateway while connected to the LAN. While Sara is out at lunch her PC is compromised via the tethered connection and corporate data is stolen. Which of the following would BEST prevent this from occurring again?

- A. Disable the wireless access and implement strict router ACLs.
- B. Reduce restrictions on the corporate web security gateway.
- C. Security policy and threat awareness training.
- D. Perform user rights and permissions reviews.

Answer: C

Explanation:

BYOD (In this case Sara's smart phone) involves the possibility of a personal device that is infected with malware introducing that malware to the network and security awareness training will address the issue of the company's security policy with regard to BYOD.

QUESTION NO: 316

Which of the following is the BEST reason to provide user awareness and training programs for organizational staff?

- A. To ensure proper use of social media
- B. To reduce organizational IT risk
- C. To detail business impact analyses
- D. To train staff on zero-days

Answer: B

Explanation:

Ideally, a security awareness training program for the entire organization should cover the following areas:

- Importance of security
- Responsibilities of people in the organization
- Policies and procedures
- Usage policies
- Account and password-selection criteria
- Social engineering prevention

You can accomplish this training either by using internal staff or by hiring outside trainers. This type of training will significantly reduce the organizational IT risk.

QUESTION NO: 317

Ann would like to forward some Personal Identifiable Information to her HR department by email, but she is worried about the confidentiality of the information. Which of the following will accomplish this task securely?

- A.** Digital Signatures
- B.** Hashing
- C.** Secret Key
- D.** Encryption

Answer: D

Explanation:

Encryption is used to prevent unauthorized users from accessing data. Data encryption will support the confidentiality of the email.

QUESTION NO: 318

Ann a technician received a spear-phishing email asking her to update her personal information by clicking the link within the body of the email. Which of the following type of training would prevent Ann and other employees from becoming victims to such attacks?

- A.** User Awareness
- B.** Acceptable Use Policy
- C.** Personal Identifiable Information
- D.** Information Sharing

Answer: C

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Employees should be made aware of this type of attack by means of training.

QUESTION NO: 319

End-user awareness training for handling sensitive personally identifiable information would include secure storage and transmission of customer:

- A. Date of birth.
- B. First and last name.
- C. Phone number.
- D. Employer name.

Answer: A

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. Date of birth is personally identifiable information.

QUESTION NO: 320

Which of the following concepts is a term that directly relates to customer privacy considerations?

- A. Data handling policies
- B. Personally identifiable information
- C. Information classification
- D. Clean desk policies

Answer: B

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. This has a direct relation to customer privacy considerations.

QUESTION NO: 321

Which of the following policies is implemented in order to minimize data loss or theft?

- A. PII handling
- B. Password policy
- C. Chain of custody
- D. Zero day exploits

Answer: A

Explanation:

Although the concept of PII is old, it has become much more important as information technology and the Internet have made it easier to collect PII through breaches of internet security, network security and web browser security, leading to a profitable market in collecting and reselling PII. PII can also be exploited by criminals to stalk or steal the identity of a person, or to aid in the planning of criminal acts.

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record.

Thus a PII handling policy can be used to protect data.

QUESTION NO: 322

Used in conjunction, which of the following are PII? (Select TWO).

- A. Marital status
- B. Favorite movie
- C. Pet's name
- D. Birthday
- E. Full name

Answer: D,E

Explanation:

Personally identifiable information (PII) is a catchall for any data that can be used to uniquely identify an individual. This data can be anything from the person's name to a fingerprint (think biometrics), credit card number, or patient record. A birthday together with a full name makes it personally identifiable information.

QUESTION NO: 323

Which of the following helps to apply the proper security controls to information?

- A. Data classification
- B. Deduplication
- C. Clean desk policy
- D. Encryption

Answer: A

Explanation:

Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. These categories make applying the appropriate policies and security controls practical.

QUESTION NO: 324

Which of the following security awareness training is BEST suited for data owners who are concerned with protecting the confidentiality of their data?

- A. Social networking use training
- B. Personally owned device policy training
- C. Tailgating awareness policy training
- D. Information classification training

Answer: D

Explanation:

Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. Knowing these categories and how to handle data according to its category is essential in protecting the confidentiality of the data.

QUESTION NO: 325

An organization is recovering data following a datacenter outage and determines that backup copies of files containing personal information were stored in an unsecure location, because the sensitivity was unknown. Which of the following activities should occur to prevent this in the future?

- A. Business continuity planning
- B. Quantitative assessment
- C. Data classification
- D. Qualitative assessment

Answer: C

Explanation:

Information classification is done by confidentiality and comprises of three categories, namely: public use, internal use and restricted use. Knowing how to apply these categories and matching it up with the appropriate data handling will address the situation of the data 'unknown sensitivity'

QUESTION NO: 326

What is the term for the process of luring someone in (usually done by an enforcement officer or a government agent)?

- A. Enticement
- B. Entrapment
- C. Deceit
- D. Sting

Answer: A

Explanation:

Enticement is the process of luring someone into your plan or trap.

QUESTION NO: 327

In which of the following categories would creating a corporate privacy policy, drafting acceptable use policies, and group based access control be classified?

- A. Security control frameworks
- B. Best practice
- C. Access control methodologies
- D. Compliance activity

Answer: B

Explanation:

Best practices are based on what is known in the industry and those methods that have consistently shown superior results over those achieved by other means. Furthermore best practices are applied to all aspects in the work environment.

QUESTION NO: 328

Which of the following is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead?

- A. Enticement
- B. Entrapment
- C. Deceit
- D. Sting

Answer: B

Explanation:

Entrapment is the process in which a law enforcement officer or a government agent encourages or induces a person to commit a crime when the potential criminal expresses a desire not to go ahead. Entrapment is a valid legal defense in a criminal prosecution.

QUESTION NO: 329

Results from a vulnerability analysis indicate that all enabled virtual terminals on a router can be accessed using the same password. The company's network device security policy mandates that at least one virtual terminal have a different password than the other virtual terminals. Which of the following sets of commands would meet this requirement?

- A. line vty 0 6 P@s5W0Rd password line vty 7 Qwer++!Y password
- B. line console 0 password password line vty 0 4 password P@s5W0Rd
- C. line vty 0 3 password Qwer++!Y line vty 4 password P@s5W0Rd
- D. line vty 0 3 password Qwer++!Y line console 0 password P@s5W0Rd

Answer: C

Explanation:

The VTY lines are the Virtual Terminal lines of the router, used solely to control inbound Telnet connections. They are virtual, in the sense that they are a function of software - there is no hardware associated with them.

Two numbers follow the keyword VTY because there is more than one VTY line for router access. The default number of lines is five on many Cisco routers. Here, I'm configuring one password for all terminal (VTY) lines. I can specify the actual terminal or VTY line numbers as a range. The syntax that you'll see most often, vty 0 4, covers all five terminal access lines.

QUESTION NO: 330

Why would a technician use a password cracker?

- A. To look for weak passwords on the network
- B. To change a user's passwords when they leave the company
- C. To enforce password complexity requirements
- D. To change users passwords if they have forgotten them

Answer: A

Explanation:

A password cracker will be able to expose weak passwords on a network.

QUESTION NO: 331

Which of the following security concepts would Sara, the security administrator, use to mitigate the risk of data loss?

- A. Record time offset
- B. Clean desk policy
- C. Cloud computing
- D. Routine log review

Answer: B

Explanation:

Clean Desk Policy Information on a desk—in terms of printouts, pads of note paper, sticky notes, and the like—can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk. This will mitigate the risk of data loss when applied.

QUESTION NO: 332

The manager has a need to secure physical documents every night, since the company began enforcing the clean desk policy. The BEST solution would include: (Select TWO).

- A. Fire- or water-proof safe.
- B. Department door locks.
- C. Proximity card.
- D. 24-hour security guard.
- E. Locking cabinets and drawers.

Answer: A,E

Explanation:

Using a safe and locking cabinets to protect backup media, documentation, and any other physical artifacts that could do harm if they fell into the wrong hands would form part of keeping employees desks clean as in a clean desk policy.

QUESTION NO: 333

XYZ Corporation is about to purchase another company to expand its operations. The CEO is concerned about information leaking out, especially with the cleaning crew that comes in at night.

The CEO would like to ensure no paper files are leaked. Which of the following is the BEST policy to implement?

- A. Social media policy
- B. Data retention policy
- C. CCTV policy
- D. Clean desk policy

Answer: D

Explanation:

Clean Desk Policy Information on a desk—in terms of printouts, pads of note paper, sticky notes, and the like—can be easily seen by prying eyes and taken by thieving hands. To protect data and your business, encourage employees to maintain clean desks and to leave out only those papers that are relevant to the project they are working on at that moment. All sensitive information should be put away when the employee is away from their desk.

QUESTION NO: 334

Which of the following could a security administrator implement to mitigate the risk of tailgating for a large organization?

- A. Train employees on correct data disposal techniques and enforce policies.

- B. Only allow employees to enter or leave through one door at specified times of the day.
- C. Only allow employees to go on break one at a time and post security guards 24/7 at each entrance.
- D. Train employees on risks associated with social engineering attacks and enforce policies.

Answer: D

Explanation:

Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. Many social engineering intruders needing physical access to a site will use this method of gaining entry. Educate users to beware of this and other social engineering ploys and prevent them from happening.

QUESTION NO: 335

Which of the following is a security concern regarding users bringing personally-owned devices that they connect to the corporate network?

- A. Cross-platform compatibility issues between personal devices and server-based applications
- B. Lack of controls in place to ensure that the devices have the latest system patches and signature files
- C. Non-corporate devices are more difficult to locate when a user is terminated
- D. Non-purchased or leased equipment may cause failure during the audits of company-owned assets

Answer: B

Explanation:

With employees who want to bring their own devices you will have to make them understand why they cannot. You do not want them plugging in a flash drive, let alone a camera, smartphone, tablet computer, or other device, on which company files could get intermingled with personal files. Allowing this to happen can create situations where data can leave the building that shouldn't as well as introduce malware to the system. Employees should not sync unauthorized smartphones to their work systems. Some smartphones use multiple wireless spectrums and unwittingly open up the possibility for an attacker in the parking lot to gain access through the phone to the internal network. Thus if you do not have controls in place then your network is definitely at risk.

QUESTION NO: 336

Several employees submit the same phishing email to the administrator. The administrator finds

that the links in the email are not being blocked by the company's security device. Which of the following might the administrator do in the short term to prevent the emails from being received?

- A. Configure an ACL
- B. Implement a URL filter
- C. Add the domain to a block list
- D. Enable TLS on the mail server

Answer: C

Explanation:

Blocking e-mail is the same as preventing the receipt of those e-mails and this is done by applying a filter. But the filter must be configured to block it. Thus you should add that specific domain from where the e-mails are being sent to the list of addresses that is to be blocked.

QUESTION NO: 337

A security researcher wants to reverse engineer an executable file to determine if it is malicious. The file was found on an underused server and appears to contain a zero-day exploit. Which of the following can the researcher do to determine if the file is malicious in nature?

- A. TCP/IP socket design review
- B. Executable code review
- C. OS Baseline comparison
- D. Software architecture review

Answer: C

Explanation:

Zero-Day Exploits begin exploiting holes in any software the very day it is discovered. It is very difficult to respond to a zero-day exploit. Often, the only thing that you as a security administrator can do is to turn off the service. Although this can be a costly undertaking in terms of productivity, it is the only way to keep the network safe. In this case you want to check if the executable file is malicious. Since a baseline represents a secure state it would be possible to check the nature of the executable file in an isolated environment against the OS baseline.

QUESTION NO: 338

A security administrator has concerns about new types of media which allow for the mass distribution of personal comments to a select group of people. To mitigate the risks involved with this media, employees should receive training on which of the following?

- A. Peer to Peer
- B. Mobile devices
- C. Social networking
- D. Personally owned devices

Answer: C

Explanation:

There many companies that allow full use of social media in the workplace, believing that the marketing opportunities it holds outweigh any loss in productivity. What they are unknowingly minimizing are the threats that exist. Rather than being all new threats, the social networking/media threats tend to fall in the categories of the same old tricks used elsewhere but in a new format. A tweet can be sent with a shortened URL so that it does not exceed the 140-character limit set by Twitter; unfortunately, the user has no idea what the shortened URL leads to. This makes training your employees regarding the risks social networking entails essential.

QUESTION NO: 339

The information security team does a presentation on social media and advises the participants not to provide too much personal information on social media web sites. This advice would BEST protect people from which of the following?

- A. Rainbow tables attacks
- B. Brute force attacks
- C. Birthday attacks
- D. Cognitive passwords attacks

Answer: D

Explanation:

Social Networking Dangers are 'amplified' in that social media networks are designed to mass distribute personal messages. If an employee reveals too much personal information it would be easy for miscreants to use the messages containing the personal information to work out possible passwords.

QUESTION NO: 340

Pete, the system administrator, has blocked users from accessing social media web sites. In addition to protecting company information from being accidentally leaked, which additional security benefit does this provide?

- A. No competition with the company's official social presence

- B. Protection against malware introduced by banner ads
- C. Increased user productivity based upon fewer distractions
- D. Elimination of risks caused by unauthorized P2P file sharing

Answer: B

Explanation:

Banner, or header information messages sent with data to find out about the system(s) does happen. Banners often identify the host, the operating system running on it, and other information that can be useful if you are going to attempt to later breach the security of it.

QUESTION NO: 341

Which of the following is a security risk regarding the use of public P2P as a method of collaboration?

- A. Data integrity is susceptible to being compromised.
- B. Monitoring data changes induces a higher cost.
- C. Users are not responsible for data usage tracking.
- D. Limiting the amount of necessary space for data storage.

Answer: A

Explanation:

Peer-to-peer (P2P) networking is commonly used to share files such as movies and music, but you must not allow users to bring in devices and create their own little networks. All networking must be done through administrators and not on a P2P basis. Data integrity can easily be compromised when using public P2P networking.

QUESTION NO: 342

Which of the following has serious security implications for large organizations and can potentially allow an attacker to capture conversations?

- A. Subnetting
- B. NAT
- C. Jabber
- D. DMZ

Answer: C

Explanation:

Jabber is a new unified communications application and could possible expose you to attackers

that want to capture conversations because Jabber provides a single interface across presence, instant messaging, voice, video messaging, desktop sharing and conferencing.

QUESTION NO: 343

The use of social networking sites introduces the risk of:

- A. Disclosure of proprietary information
- B. Data classification issues
- C. Data availability issues
- D. Broken chain of custody

Answer: A

Explanation:

People and processes must be in place to prevent the unauthorized disclosure of proprietary information and sensitive information as these pose a security risk to companies. With social networking your company can be exposed to as many threats as the amount of users that make use of social networking and are not advised on security policy regarding the use of social networking.

QUESTION NO: 344

Which of the following statements is MOST likely to be included in the security awareness training about P2P?

- A. P2P is always used to download copyrighted material.
- B. P2P can be used to improve computer system response.
- C. P2P may prevent viruses from entering the network.
- D. P2P may cause excessive network bandwidth.

Answer: D

Explanation:

P2P networking by definition involves networking which will reduce available bandwidth for the rest of the users on the network.

QUESTION NO: 345

A security team has established a security awareness program. Which of the following would BEST prove the success of the program?

- A. Policies
- B. Procedures
- C. Metrics
- D. Standards

Answer: C

Explanation:

All types of training should be followed up- be tested to see if it worked and how much was learned in the training process. You must follow up and gather training metrics to validate compliance and security posture. By training metrics, we mean some quantifiable method for determining the efficacy of training.

QUESTION NO: 346

Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

- A. CCTV system access
- B. Dial-up access
- C. Changing environmental controls
- D. Ping of death

Answer: C

Explanation:

Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant. A computer room will typically require full-time environmental control. Changing any of these controls (when it was set to its optimum values) will result in damage.

QUESTION NO: 347

A company that purchased an HVAC system for the datacenter is MOST concerned with which of the following?

- A. Availability
- B. Integrity

- C. Confidentiality
- D. Fire suppression

Answer: A

Explanation:

Availability means simply to make sure that the data and systems are available for authorized users. Data backups, redundant systems, and disaster recovery plans all support availability; as does environmental support by means of HVAC.

QUESTION NO: 348

Which of the following should be connected to the fire alarm system in order to help prevent the spread of a fire in a server room without data loss to assist in an FM-200 deployment?

- A. Water base sprinkler system
- B. Electrical
- C. HVAC
- D. Video surveillance

Answer: C

Explanation:

HVAC refers to heating, ventilation and air-conditioning to allow for a zone-based environmental control measure. The fire-alarm system should ideally also be hooked up to the HVAC so that the HVAC can monitor the changes in heating and ventilation.

QUESTION NO: 349

Which of the following is a security benefit of providing additional HVAC capacity or increased tonnage in a datacenter?

- A. Increased availability of network services due to higher throughput
- B. Longer MTBF of hardware due to lower operating temperatures
- C. Higher data integrity due to more efficient SSD cooling
- D. Longer UPS run time due to increased airflow

Answer: B

Explanation:

The mean time between failures (MTBF) is the measure of the anticipated incidence of failure for a system or component. This measurement determines the component's anticipated lifetime. If the MTBF of a cooling system is one year, you can anticipate that the system will last for a one-year

period; this means that you should be prepared to replace or rebuild the system once a year. If the system lasts longer than the MTBF, your organization receives a bonus. MTBF is helpful in evaluating a system's reliability and life expectancy. Thus longer MTBF due to lower operating temperatures is a definite advantage

QUESTION NO: 350

Which of the following fire suppression systems is MOST likely used in a datacenter?

- A. FM-200
- B. Dry-pipe
- C. Wet-pipe
- D. Vacuum

Answer: A

Explanation:

FM200 is a gas and the principle of a gas system is that it displaces the oxygen in the room, thereby removing this essential component of a fire. In a data center it is the preferred choice of fire suppressant.

QUESTION NO: 351

When implementing fire suppression controls in a datacenter it is important to:

- A. Select a fire suppression system which protects equipment but may harm technicians.
- B. Ensure proper placement of sprinkler lines to avoid accidental leakage onto servers.
- C. Integrate maintenance procedures to include regularly discharging the system.
- D. Use a system with audible alarms to ensure technicians have 20 minutes to evacuate.

Answer: B

Explanation:

Water-based systems can cause serious damage to all electrical equipment and the sprinkler lines in a fire suppression control system should be placed in such a way so as not to leak onto computers when it does get activated because it works with overhead nozzles.

QUESTION NO: 352

Which of the following should be considered to mitigate data theft when using CAT5 wiring?

- A. CCTV
- B. Environmental monitoring
- C. Multimode fiber
- D. EMI shielding

Answer: D

Explanation:

EMI Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. Thus all wiring should be shielded to mitigate data theft.

QUESTION NO: 353

Environmental control measures include which of the following?

- A. Access list
- B. Lighting
- C. Motion detection
- D. EMI shielding

Answer: D

Explanation:

Environmental controls include HVAC, Fire Suppression, EMI Shielding, Hot and Cold Aisles, Environmental monitoring as well as Temperature and Humidity controls.

QUESTION NO: 354

When a new network drop was installed, the cable was run across several fluorescent lights. The users of the new network drop experience intermittent connectivity. Which of the following environmental controls was MOST likely overlooked during installation?

- A. Humidity sensors
- B. EMI shielding
- C. Channel interference
- D. Cable kinking

Answer: B

Explanation:

Shielding refers to the process of preventing electronic emissions from your computer systems from being used to gather intelligence and preventing outside electronic emissions from disrupting your information-processing abilities. In this case you are experiencing intermittent connectivity since Electro Magnetic Interference (EMI) was not taken into account when running the cables over fluorescent lighting.

QUESTION NO: 355

The datacenter design team is implementing a system, which requires all servers installed in racks to face in a predetermined direction. AN infrared camera will be used to verify that servers are properly racked. Which of the following datacenter elements is being designed?

- A. Hot and cold aisles
- B. Humidity control
- C. HVAC system
- D. EMI shielding

Answer: A

Explanation:

There are often multiple rows of servers located in racks in server rooms. The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles. With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation.

Infrared cameras are heat detection measures thus it is hot and cold aisle design elements.

QUESTION NO: 356

Which of the following is an effective way to ensure the BEST temperature for all equipment within a datacenter?

- A. Fire suppression
- B. Raised floor implementation
- C. EMI shielding
- D. Hot or cool aisle containment

Answer: D

Explanation:

There are often multiple rows of servers located in racks in server rooms. The rows of servers are known as aisles, and they can be cooled as hot aisles and cold aisles. With a hot aisle, hot air outlets are used to cool the equipment, whereas with cold aisles, cold air intake is used to cool the equipment. Combining the two, you have cold air intake from below the aisle and hot air outtake above it, providing constant circulation. This is a more effective way of controlling temperature to safeguard your equipment in a data center.

QUESTION NO: 357

Which of the following results in datacenters with failed humidity controls? (Select TWO).

- A. Excessive EMI
- B. Electrostatic charge
- C. Improper ventilation
- D. Condensation
- E. Irregular temperature

Answer: B,D

Explanation:

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock. Most environmental systems also regulate humidity; however, a malfunctioning system can cause the humidity to be almost entirely extracted from a room. Make sure that environmental systems are regularly serviced. Electrostatic damage can occur when humidity levels get too low. Condensation is a direct result from failed humidity levels.

QUESTION NO: 358

The datacenter manager is reviewing a problem with a humidity factor that is too low. Which of the following environmental problems may occur?

- A. EMI emanations
- B. Static electricity
- C. Condensation
- D. Dry-pipe fire suppression

Answer: B

Explanation:

Humidity control prevents the buildup of static electricity in the environment. If the humidity drops

much below 50 percent, electronic components are extremely vulnerable to damage from electrostatic shock.

QUESTION NO: 359

A technician is investigating intermittent switch degradation. The issue only seems to occur when the building's roof air conditioning system runs. Which of the following would reduce the connectivity issues?

- A. Adding a heat deflector
- B. Redundant HVAC systems
- C. Shielding
- D. Add a wireless network

Answer: C

Explanation:

EMI can cause circuit overload, spikes, or even electrical component failure. In the question it is mentioned that switch degradation occurs when the building's roof air-conditioning system is also running. All electromechanical systems emanate EMI. Thus you could alleviate the problem using EMI shielding.

QUESTION NO: 360 DRAG DROP

Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.

Types of Security

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.



1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus

Mobile Device Security	Server in Data Center Security

Answer:

Types of Security

Task: Drag the items on the left to show the different types of security for the shown devices. Not all fields need to be filled. Not all items need to be used.



1. GPS Tracking
2. Mantrap
3. Remote wipe
4. Strong Passwords
5. Cable lock
6. Biometrics
7. Proximity Badges
8. FM-200
9. HVAC
10. Device Encryption
11. Antivirus

Mobile Device Security	Server in Data Center Security
1. GPS Tracking	8. FM-200
3. Remote wipe	6. Biometrics
10. Device Encryption	7. Proximity Badges
4. Strong Passwords	2. Mantrap

Explanation:

Mobile Device Security

GPS tracking

Remote wipe

Device Encryption

Strong password

Server in Data Center Security

FM-200

Biometrics

Proximity Badges

Mantrap

For mobile devices, at bare minimum you should have the following security measures in place: Screen lock, Strong password, Device encryption, Remote wipe/Sanitation, voice encryption, GPS tracking, Application control, Storage segmentation, Asset tracking as well as Device Access control.

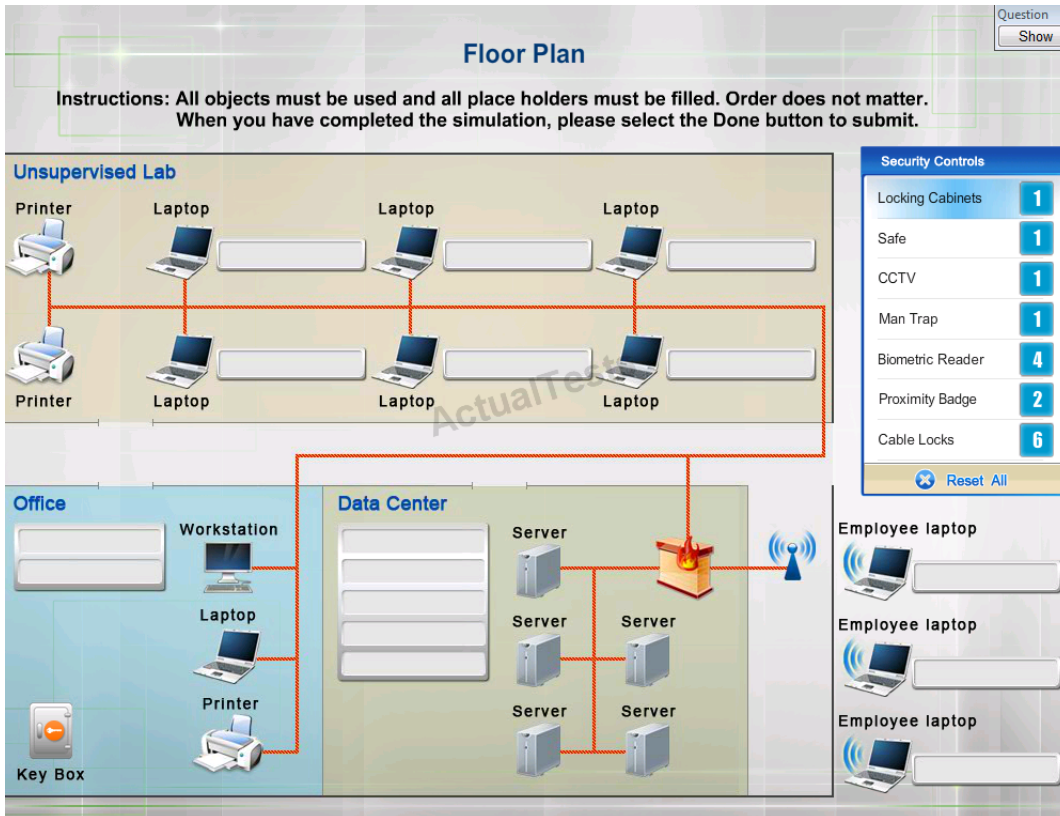
For servers in a data center your security should include: Fire extinguishers such as FM200 as part of fire suppression; Biometric, proximity badges, mantraps, HVAC, cable locks; these can all be physical security measures to control access to the server.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 418

QUESTION NO: 361 CORRECT TEXT

You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan-Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.



Answer: <map><m x1="809" x2="944" y1="163" y2="198" ss="0" a="0" /><m x1="804" x2="945" y1="205" y2="232" ss="0" a="0" /><m x1="805" x2="944" y1="239" y2="269" ss="0" a="0" /><m x1="807" x2="944" y1="277" y2="310" ss="0" a="0" /><m x1="803" x2="946" y1="317" y2="345" ss="0" a="0" /><m x1="804" x2="947" y1="349" y2="380" ss="0" a="0" /><m x1="810" x2="945" y1="389" y2="422" ss="0" a="0" /><m x1="200" x2="334" y1="221" y2="245" ss="1" a="0" /><m x1="410" x2="548" y1="221" y2="247" ss="1" a="0" /><m x1="621" x2="758" y1="222" y2="247" ss="1" a="0" /><m x1="621" x2="755" y1="323" y2="347" ss="1" a="0" /><m x1="410" x2="551" y1="321" y2="348" ss="1" a="0" /><m x1="202" x2="338" y1="324" y2="351" ss="1" a="0" /><m x1="8" x2="150" y1="488" y2="513" ss="1" a="0" /><m x1="11" x2="147" y1="519" y2="546" ss="1" a="0" /><m x1="311" x2="448" y1="489" y2="513" ss="1" a="0" /><m x1="313" x2="450" y1="518" y2="541" ss="1" a="0" /><m x1="315" x2="451" y1="547" y2="570" ss="1" a="0" /><m x1="316" x2="449" y1="574" y2="597" ss="1" a="0" /><m x1="315" x2="449" y1="603" y2="629" ss="1" a="0" /><m x1="851" x2="986" y1="522" y2="550" ss="1" a="0" /><m x1="849" x2="986" y1="612" y2="640" ss="1" a="0" /><m x1="853" x2="987" y1="701" y2="727" ss="1" a="0" /><c start="6" stop="0" /><c start="6" stop="1" /><c start="6" stop="2" /><c start="6" stop="3" /><c start="6" stop="4" /><c start="6" stop="5" /><c start="5" stop="6" /><c start="1" stop="7" /><c start="2" stop="8" /><c start="5" stop="9" /><c start="3" stop="10" /><c start="0" stop="11" /><c start="4" stop="12" /><c start="4" stop="13" /><c start="4" stop="14" /><c start="4" stop="15" /></map>

Explanation:

Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away

Proximity badge + reader

Safe is a hardware/physical security measure

Mantrap can be used to control access to sensitive areas.

CCTV can be used as video surveillance.

Biometric reader can be used to control and prevent unauthorized access.

Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 369

QUESTION NO: 362

A malicious person gained access to a datacenter by ripping the proximity badge reader off the wall near the datacenter entrance. This caused the electronic locks on the datacenter door to release because the:

- A.** badge reader was improperly installed.
- B.** system was designed to fail open for life-safety.
- C.** system was installed in a fail closed configuration.
- D.** system used magnetic locks and the locks became demagnetized.

Answer: B

Explanation:

It describes a design the lock to fail open for life safety, causing the door to stay open when power is lost – in this case the proximity badge reader was ripped off the wall.

QUESTION NO: 363

A company is trying to implement physical deterrent controls to improve the overall security posture of their data center. Which of the following BEST meets their goal?

- A.** Visitor logs
- B.** Firewall
- C.** Hardware locks
- D.** Environmental monitoring

Answer: C

Explanation:

Hardware security involves applying physical security modifications to secure the system(s) and preventing them from leaving the facility. Don't spend all of your time worrying about intruders coming through the network wire while overlooking the obvious need for physical security.

Hardware security involves the use of locks to prevent someone from picking up and carrying out your equipment.

QUESTION NO: 364

Pete, an IT Administrator, needs to secure his server room. Which of the following mitigation methods would provide the MOST physical protection?

- A. Sign in and sign out logs
- B. Mantrap
- C. Video surveillance
- D. HVAC

Answer: B**Explanation:**

Mantraps are designed to contain an unauthorized, potentially hostile person/individual physically until authorities arrive. Mantraps are typically manufactured with bulletproof glass, high-strength doors, and locks and to allow the minimal amount of individuals depending on its size. Some mantraps even include scales that will weigh the person. The doors are designed in such a way as to open only when the mantrap is occupied or empty and not in-between. This means that the backdoor must first close before the front door will open. Mantraps are in most cases also combined with guards. This is the most physical protection any one measure will provide.

QUESTION NO: 365

Visitors entering a building are required to close the back door before the front door of the same entry room is open. Which of the following is being described?

- A. Tailgating
- B. Fencing
- C. Screening
- D. Mantrap

Answer: D**Explanation:**

Mantraps are designed to contain an unauthorized, potentially hostile person/individual physically until authorities arrive. Mantraps are typically manufactured with bulletproof glass, high-strength doors, and locks and to allow the minimal amount of individuals depending on its size. Some mantraps even include scales that will weigh the person. The doors are designed in such a way as to open only when the mantrap is occupied or empty and not in-between. This means that the backdoor must first close before the front door will open; exactly what is required in this scenario.

QUESTION NO: 366

A company is installing a new security measure that would allow one person at a time to be authenticated to an area without human interaction. Which of the following does this describe?

- A. Fencing
- B. Mantrap
- C. A guard
- D. Video surveillance

Answer: B

Explanation:

Mantraps make use of electronic locks and are designed to allow you to limit the amount of individual allowed access to an area at any one time.

QUESTION NO: 367

Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?

- A. Bollards
- B. Video surveillance
- C. Proximity readers
- D. Fencing

Answer: B

Explanation:

Video surveillance is making use of a camera, or CCTV that is able to record everything it sees and is always running. This way you will be able to check exactly who enters secure areas.

QUESTION NO: 368

A datacenter requires that staff be able to identify whether or not items have been removed from the facility. Which of the following controls will allow the organization to provide automated notification of item removal?

- A. CCTV
- B. Environmental monitoring
- C. RFID
- D. EMI shielding

Answer: C

Explanation:

RFID is radio frequency identification that works with readers that work with 13.56 MHz smart cards and 125 kHz proximity cards and can open turnstiles, gates, and any other physical security safeguards once the signal is read. Fitting out the equipment with RFID will allow you to provide automated notification of item removal in the event of any of the equipped items is taken off the premises.

QUESTION NO: 369

Datacenter access is controlled with proximity badges that record all entries and exits from the datacenter. The access records are used to identify which staff members accessed the data center in the event of equipment theft. Which of the following **MUST** be prevented in order for this policy to be effective?

- A. Password reuse
- B. Phishing
- C. Social engineering
- D. Tailgating

Answer: D

Explanation:

Tailgating is the term used for someone being so close to you when you enter a building that they are able to come in right behind you without needing to use a key, a card, or any other security device. This should be prevented in this case.

QUESTION NO: 370

Due to issues with building keys being duplicated and distributed, a security administrator wishes to change to a different security control regarding a restricted area. The goal is to provide access based upon facial recognition. Which of the following will address this requirement?

- A. Set up mantraps to avoid tailgating of approved users.
- B. Place a guard at the entrance to approve access.
- C. Install a fingerprint scanner at the entrance.
- D. Implement proximity readers to scan users' badges.

Answer: B

Explanation:

A guard can be instructed to deny access until authentication has occurred will address the situation adequately.

QUESTION NO: 371

A security administrator wants to deploy a physical security control to limit an individual's access into a sensitive area. Which of the following should be implemented?

- A. Guards
- B. CCTV
- C. Bollards
- D. Spike strip

Answer: A

Explanation:

A guard can be intimidating and respond to a situation and in a case where you want to limit an individual's access to a sensitive area a guard would be the most effective.

QUESTION NO: 372

After running into the data center with a vehicle, attackers were able to enter through the hole in the building and steal several key servers in the ensuing chaos. Which of the following security measures can be put in place to mitigate the issue from occurring in the future?

- A. Fencing
- B. Proximity readers
- C. Video surveillance

D. Bollards

Answer: D

Explanation:

To stop someone from entering a facility, barricades or gauntlets can be used. These are often used in conjunction with guards, fencing, and other physical security measures. Bollards are physical barriers that are strong enough to withstand impact with a vehicle.

QUESTION NO: 373

A system administrator has concerns regarding their users accessing systems and secured areas using others' credentials. Which of the following can BEST address this concern?

- A.** Create conduct policies prohibiting sharing credentials.
- B.** Enforce a policy shortening the credential expiration timeframe.
- C.** Implement biometric readers on laptops and restricted areas.
- D.** Install security cameras in areas containing sensitive systems.

Answer: C

Explanation:

Biometrics is an authentication process that makes use of physical characteristics to establish identification. This will prevent users making use of others credentials.

QUESTION NO: 374

Which of the following preventative controls would be appropriate for responding to a directive to reduce the attack surface of a specific host?

- A.** Installing anti-malware
- B.** Implementing an IDS
- C.** Taking a baseline configuration
- D.** Disabling unnecessary services

Answer: D

Explanation:

Preventive controls are to stop something from happening. These can include locked doors that keep intruders out, user training on potential harm (to keep them vigilant and alert), or even biometric devices and guards that deny access until authentication has occurred. By disabling all unnecessary services you would be reducing the attack surface because then there is less opportunity for risk incidents to happen. There are many risks with having many services enabled

since a service can provide an attack vector that someone could exploit against your system. It is thus best practice to enable only those services that are absolutely required.

QUESTION NO: 375

Joe, the system administrator, has been asked to calculate the Annual Loss Expectancy (ALE) for a \$5,000 server, which often crashes. In the past year, the server has crashed 10 times, requiring a system reboot to recover with only 10% loss of data or function. Which of the following is the ALE of this server?

- A. \$500
- B. \$5,000
- C. \$25,000
- D. \$50,000

Answer: B

Explanation:

$SLE \times ARO = ALE$, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

$$(5000 \times 10) \times 0.1 = 5000$$

QUESTION NO: 376

Sara, a security analyst, is trying to prove to management what costs they could incur if their customer database was breached. This database contains 250 records with PII. Studies show that the cost per record for a breach is \$300. The likelihood that their database would be breached in the next year is only 5%. Which of the following is the ALE that Sara should report to management for a security breach?

- A. \$1,500
- B. \$3,750
- C. \$15,000
- D. \$75,000

Answer: B

Explanation:

$SLE \times ARO = ALE$, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

$$SLE = 250 \times \$300; ARO = 5\%$$

$$\$75000 \times 0.05 = \$3750$$

QUESTION NO: 377

An advantage of virtualizing servers, databases, and office applications is:

- A. Centralized management.
- B. Providing greater resources to users.
- C. Stronger access control.
- D. Decentralized management.

Answer: A

Explanation:

Virtualization consists of allowing one set of hardware to host multiple virtual Machines and in the case of software and applications; one host is all that is required. This makes centralized management a better prospect.

QUESTION NO: 378

Key elements of a business impact analysis should include which of the following tasks?

- A. Develop recovery strategies, prioritize recovery, create test plans, post-test evaluation, and update processes.
- B. Identify institutional and regulatory reporting requirements, develop response teams and communication trees, and develop press release templates.
- C. Employ regular preventive measures such as patch management, change management, antivirus and vulnerability scans, and reports to management.
- D. Identify critical assets systems and functions, identify dependencies, determine critical downtime limit, define scenarios by type and scope of impact, and quantify loss potential.

Answer: D

Explanation:

The key components of a Business impact analysis (BIA) include:

Identifying Critical Functions

Prioritizing Critical Business Functions

Calculating a Timeframe for Critical Systems Loss

Estimating the Tangible and Intangible Impact on the Organization

QUESTION NO: 379

A security administrator is tasked with calculating the total ALE on servers. In a two year period of time, a company has to replace five servers. Each server replacement has cost the company

\$4,000 with downtime costing \$3,000. Which of the following is the ALE for the company?

- A. \$7,000
- B. \$10,000
- C. \$17,500
- D. \$35,000

Answer: C

Explanation:

$SLE \times ARO = ALE$, where SLE is equal to asset value (AV) times exposure factor (EF); and ARO is the annualized rate of occurrence.

$$SLE = (\$4000 + \$3000) \times 5 = \$35000$$

$$ARO = 2 \text{ years} \text{ Thus per year it would be } 50\% = 0.5$$

$$\text{The ALE is thus } \$35000 \times 0.5 = \$17500$$

QUESTION NO: 380

In the case of a major outage or business interruption, the security office has documented the expected loss of earnings, potential fines and potential consequence to customer service. Which of the following would include the MOST detail on these objectives?

- A. Business Impact Analysis
- B. IT Contingency Plan
- C. Disaster Recovery Plan
- D. Continuity of Operations

Answer: A

Explanation:

Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

QUESTION NO: 381

Which of the following would BEST be used to calculate the expected loss of an event, if the likelihood of an event occurring is known? (Select TWO).

- A. DAC
- B. ALE
- C. SLE
- D. ARO
- E. ROI

Answer: B,C

Explanation:

ALE (Annual Loss Expectancy) is equal to the SLE (Single Loss Expectancy) times the annualized rate of occurrence. SLE (Single Loss Expectancy) is equal to asset value (AV) times exposure factor (EF).

QUESTION NO: 382

A company's chief information officer (CIO) has analyzed the financial loss associated with the company's database breach. They calculated that one single breach could cost the company \$1,000,000 at a minimum. Which of the following documents is the CIO MOST likely updating?

- A. Succession plan
- B. Continuity of operation plan
- C. Disaster recovery plan
- D. Business impact analysis

Answer: D

Explanation:

Business impact analysis (BIA) is the process of evaluating all of the critical systems in an organization to define impact and recovery plans. BIA isn't concerned with external threats or vulnerabilities; the analysis focuses on the impact a loss would have on the organization. A BIA comprises the following: identifying critical functions, prioritizing critical business functions, calculating a timeframe for critical systems loss, and estimating the tangible impact on the organization.

QUESTION NO: 383

A network administrator has recently updated their network devices to ensure redundancy is in place so that:

- A. switches can redistribute routes across the network.
- B. environmental monitoring can be performed.
- C. single points of failure are removed.

D. hot and cold aisles are functioning.

Answer: C

Explanation:

Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction. The best way to remove an SPOF from your environment is to add redundancy.

QUESTION NO: 384

After an assessment, auditors recommended that an application hosting company should contract with additional data providers for redundant high speed Internet connections. Which of the following is MOST likely the reason for this recommendation? (Select TWO).

- A. To allow load balancing for cloud support
- B. To allow for business continuity if one provider goes out of business
- C. To eliminate a single point of failure
- D. To allow for a hot site in case of disaster
- E. To improve intranet communication speeds

Answer: B,C

Explanation:

A high-speed internet connection to a second data provider could be used to keep an up-to-date replicate of the main site. In case of problem on the first site, operation can quickly switch to the second site. This eliminates the single point of failure and allows the business to continue uninterrupted on the second site.

Note: Recovery Time Objective

The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during BIA creation.

QUESTION NO: 385

Which of the following utilities can be used in Linux to view a list of users' failed authentication attempts?

- A. badlog
- B. faillog
- C. wronglog
- D. killlog

Answer: B

Explanation:

var/log/faillog - This Linux log file contains failed user logins. You'll find this log useful when tracking attempts to crack into your system.

/var/log/apport.log This log records application crashes. Sometimes these can reveal attempts to compromise the system or the presence of a virus or spyware.

QUESTION NO: 386

Which of the following risks could IT management be mitigating by removing an all-in-one device?

- A. Continuity of operations
- B. Input validation
- C. Single point of failure
- D. Single sign on

Answer: C

Explanation:

The major disadvantage of combining everything into one, although you do this to save costs, is to include a potential single point of failure and the reliance/dependence on a single vendor.

QUESTION NO: 387

Which of the following risk concepts requires an organization to determine the number of failures per year?

- A. SLE
- B. ALE
- C. MTBF
- D. Quantitative analysis

Answer: B

Explanation:

ALE is the annual loss expectancy value. This is a monetary measure of how much loss you could expect in a year.

QUESTION NO: 388

Upper management decides which risk to mitigate based on cost. This is an example of:

- A. Qualitative risk assessment
- B. Business impact analysis
- C. Risk management framework
- D. Quantitative risk assessment

Answer: D

Explanation:

Quantitative analysis / assessment is used to show the logic and cost savings in replacing a server for example before it fails rather than after the failure. Quantitative assessments assign a dollar amount.

QUESTION NO: 389

Corporate IM presents multiple concerns to enterprise IT. Which of the following concerns should Jane, the IT security manager, ensure are under control? (Select THREE).

- A. Authentication
- B. Data leakage
- C. Compliance
- D. Malware
- E. Non-repudiation
- F. Network loading

Answer: B,C,D

Explanation:

In a joint enterprise, data may be combined from both organizations. It must be determined, in advance, who is responsible for that data and how the data backups will be managed. Data leakage, compliance and Malware issues are all issues concerning data ownership and backup which are both impacted on by corporate IM.

QUESTION NO: 390

Which of the following is being tested when a company's payroll server is powered off for eight hours?

- A. Succession plan
- B. Business impact document
- C. Continuity of operations plan

D. Risk assessment plan**Answer: C****Explanation:**

Continuity of operations plan is the effort to ensure the continued performance of critical business functions during a wide range of potential emergencies.

QUESTION NO: 391

A security administrator is reviewing the company's continuity plan. The plan specifies an RTO of six hours and RPO of two days. Which of the following is the plan describing?

- A.** Systems should be restored within six hours and no later than two days after the incident.
- B.** Systems should be restored within two days and should remain operational for at least six hours.
- C.** Systems should be restored within six hours with a minimum of two days worth of data.
- D.** Systems should be restored within two days with a minimum of six hours worth of data.

Answer: C**Explanation:**

The recovery time objective (RTO) is the maximum amount of time that a process or service is allowed to be down and the consequences still to be considered acceptable. Beyond this time, the break in business continuity is considered to affect the business negatively. The RTO is agreed on during the business impact analysis (BIA) creation.

The recovery point objective (RPO) is similar to RTO, but it defines the point at which the system needs to be restored. This could be where the system was two days before it crashed (whip out the old backup tapes) or five minutes before it crashed (requiring complete redundancy). As a general rule, the closer the RPO matches the item of the crash, the more expensive it is to obtain.

QUESTION NO: 392

Pete, the system administrator, is reviewing his disaster recovery plans. He wishes to limit the downtime in the event of a disaster, but does not have the budget approval to implement or maintain an offsite location that ensures 99.99% availability. Which of the following would be Pete's BEST option?

- A.** Use hardware already at an offsite location and configure it to be quickly utilized.
- B.** Move the servers and data to another part of the company's main campus from the server room.
- C.** Retain data back-ups on the main campus and establish redundant servers in a virtual

environment.

D. Move the data back-ups to the offsite location, but retain the hardware on the main campus for redundancy.

Answer: A

Explanation:

A warm site provides some of the capabilities of a hot site, but it requires the customer to do more work to become operational. Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement.

Warm sites may be for your exclusive use, but they don't have to be. A warm site requires more advanced planning, testing, and access to media for system recovery. Warm sites represent a compromise between a hot site, which is very expensive, and a cold site, which isn't preconfigured.

QUESTION NO: 393

Ann is starting a disaster recovery program. She has gathered specifics and team members for a meeting on site. Which of the following types of tests is this?

- A.** Structured walkthrough
- B.** Full Interruption test
- C.** Checklist test
- D.** Tabletop exercise

Answer: A

Explanation:

A structured walkthrough test of a recovery plan involves representatives from each of the functional areas coming together to review the plan to determine if the plan pertaining to their area is accurate and complete and can be implemented when required.

QUESTION NO: 394

When a communications plan is developed for disaster recovery and business continuity plans, the MOST relevant items to include would be: (Select TWO).

- A.** Methods and templates to respond to press requests, institutional and regulatory reporting requirements.

- B.** Methods to exchange essential information to and from all response team members, employees, suppliers, and customers.
- C.** Developed recovery strategies, test plans, post-test evaluation and update processes.
- D.** Defined scenarios by type and scope of impact and dependencies, with quantification of loss potential.
- E.** Methods to review and report on system logs, incident response, and incident handling.

Answer: A,B

Explanation:

A: External emergency communications that should fit into your business continuity plan include notifying family members of an injury or death, discussing the disaster with the media, and providing status information to key clients and stakeholders. Each message needs to be prepared with the audience (e.g., employees, media, families, government regulators) in mind; broad general announcements may be acceptable in the initial aftermath of an incident, but these will need to be tailored to the audiences in subsequent releases.

B: A typical emergency communications plan should be extensive in detail and properly planned by a business continuity planner. Internal alerts are sent using either email, overhead building paging systems, voice messages or text messages to cell/smartphones with instructions to evacuate the building and relocate at assembly points, updates on the status of the situation, and notification of when it's safe to return to work.

QUESTION NO: 395

After a production outage, which of the following documents contains detailed information on the order in which the system should be restored to service?

- A.** Succession planning
- B.** Disaster recovery plan
- C.** Information security plan
- D.** Business impact analysis

Answer: B

Explanation:

A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

QUESTION NO: 396

Which of the following concepts defines the requirement for data availability?

- A. Authentication to RADIUS
- B. Non-repudiation of email messages
- C. Disaster recovery planning
- D. Encryption of email messages

Answer: C

Explanation:

A disaster-recovery plan, or scheme, helps an organization respond effectively when a disaster occurs. Disasters may include system failure, network failure, infrastructure failure, and natural disaster. The primary emphasis of such a plan is reestablishing services and minimizing losses.

QUESTION NO: 397

Which of the following is the MOST specific plan for various problems that can arise within a system?

- A. Business Continuity Plan
- B. Continuity of Operation Plan
- C. Disaster Recovery Plan
- D. IT Contingency Plan

Answer: D

Explanation:

An IT contingency plan would focus on the IT aspect in particular to ensure business continuity.

QUESTION NO: 398

Joe, the system administrator, is performing an overnight system refresh of hundreds of user computers. The refresh has a strict timeframe and must have zero downtime during business hours. Which of the following should Joe take into consideration?

- A. A disk-based image of every computer as they are being replaced.
- B. A plan that skips every other replaced computer to limit the area of affected users.
- C. An offsite contingency server farm that can act as a warm site should any issues appear.
- D. A back-out strategy planned out anticipating any unforeseen problems that may arise.

Answer: D

Explanation:

A backout is a reversion from a change that had negative consequences. It could be, for example, that everything was working fine until you installed a service pack on a production machine, and

then services that were normally available were no longer accessible. The backout, in this instance, would revert the system to the state that it was in before the service pack was applied. Backout plans can include uninstalling service packs, hotfixes, and patches, but they can also include reversing a migration and using previous firmware. A key component to creating such a plan is identifying what events will trigger your implementing the backout.

QUESTION NO: 399

Which of the following concepts is BEST described as developing a new chain of command in the event of a contingency?

- A. Business continuity planning
- B. Continuity of operations
- C. Business impact analysis
- D. Succession planning

Answer: D

Explanation:

Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

QUESTION NO: 400

Pete, the Chief Executive Officer (CEO) of a company, has increased his travel plans for the next two years to improve business relations. Which of the following would need to be in place in case something happens to Pete?

- A. Succession planning
- B. Disaster recovery
- C. Separation of duty
- D. Removing single loss expectancy

Answer: A

Explanation:

Succession planning outlines those internal to the organization who have the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure

that they are up to speed when it comes time for them to fill those positions.

QUESTION NO: 401

Establishing a published chart of roles, responsibilities, and chain of command to be used during a disaster is an example of which of the following?

- A. Fault tolerance
- B. Succession planning
- C. Business continuity testing
- D. Recovery point objectives

Answer: B

Explanation:

Succession planning outlines those internal to the organization that has the ability to step into positions when they open. By identifying key roles that cannot be left unfilled and associating internal employees who can step into these roles, you can groom those employees to make sure that they are up to speed when it comes time for them to fill those positions.

QUESTION NO: 402

A network administrator recently updated various network devices to ensure redundancy throughout the network. If an interface on any of the Layer 3 devices were to go down, traffic will still pass through another interface and the production environment would be unaffected. This type of configuration represents which of the following concepts?

- A. High availability
- B. Load balancing
- C. Backout contingency plan
- D. Clustering

Answer: A

Explanation:

High availability (HA) refers to the measures used to keep services and systems operational during an outage. In short, the goal is to provide all services to all users, where they need them and when they need them. With high availability, the goal is to have key services available 99.999 percent of the time (also known as five nines availability).

QUESTION NO: 403

A network administrator has purchased two devices that will act as failovers for each other. Which of the following concepts does this BEST illustrate?

- A. Authentication
- B. Integrity
- C. Confidentiality
- D. Availability

Answer: D

Explanation:

Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored. In the case of a network, this means processing switches to another network path in the event of a network failure in the primary path. This means availability.

QUESTION NO: 404

The main corporate website has a service level agreement that requires availability 100% of the time, even in the case of a disaster. Which of the following would be required to meet this demand?

- A. Warm site implementation for the datacenter
- B. Geographically disparate site redundant datacenter
- C. Localized clustering of the datacenter
- D. Cold site implementation for the datacenter

Answer: B

Explanation:

Data backups, redundant systems, and disaster recovery plans all support availability. AN in this case a geographically disparate site redundant datacenter represents 100% availability regardless of whether a disaster event occurs.

QUESTION NO: 405

A company replaces a number of devices with a mobile appliance, combining several functions. Which of the following descriptions fits this new implementation? (Select TWO).

- A. Cloud computing
- B. Virtualization
- C. All-in-one device
- D. Load balancing
- E. Single point of failure

Answer: C,E

Explanation:

The disadvantages of combining everything into one include a potential single point of failure, and the dependence on the one vendor. The all –in-one device represents a single point of failure risk being taken on.

QUESTION NO: 406

A small business needs to incorporate fault tolerance into their infrastructure to increase data availability. Which of the following options would be the BEST solution at a minimal cost?

- A. Clustering
- B. Mirrored server
- C. RAID
- D. Tape backup

Answer: C

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

QUESTION NO: 407

Which of the following may significantly reduce data loss if multiple drives fail at the same time?

- A. Virtualization
- B. RAID
- C. Load balancing
- D. Server clustering

Answer: B

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning.

QUESTION NO: 408

Which of the following provides data the best fault tolerance at the LOWEST cost?

- A. Load balancing
- B. Clustering
- C. Server virtualization
- D. RAID 6

Answer: D

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID can achieve fault tolerance using software which can be done using the existing hardware and software thus representing the lowest cost option.

QUESTION NO: 409

Which of the following provides the LEAST availability?

- A. RAID 0
- B. RAID 1
- C. RAID 3
- D. RAID 5

Answer: A

Explanation:

RAID, or redundant array of independent disks (RAID). RAID allows your existing servers to have more than one hard drive so that if the main hard drive fails, the system keeps functioning. RAID 0 is disk striping. It uses multiple drives and maps them together as a single physical drive. This is done primarily for performance, not for fault tolerance. If any drive in a RAID 0 array fails, the entire logical drive becomes unusable.

QUESTION NO: 410

Which of the following can Pete, a security administrator, use to distribute the processing effort when generating hashes for a password cracking program?

- A. RAID
- B. Clustering
- C. Redundancy
- D. Virtualization

Answer: B

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy.

Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

QUESTION NO: 411

Sara, a security architect, has developed a framework in which several authentication servers work together to increase processing power for an application. Which of the following does this represent?

- A. Warm site
- B. Load balancing
- C. Clustering
- D. RAID

Answer: C

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy.

Server clustering is used to provide failover capabilities / redundancy in addition to scalability as demand increases.

QUESTION NO: 412

Which of the following concepts allows an organization to group large numbers of servers together in order to deliver a common service?

- A. Clustering
- B. RAID
- C. Backup Redundancy
- D. Cold site

Answer: A

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

Clustering is done whenever you connect multiple computers to work and act together as a single server. It is meant to utilize parallel processing and can also add to redundancy.

QUESTION NO: 413

Jane has implemented an array of four servers to accomplish one specific task. This is BEST known as which of the following?

- A. Clustering
- B. RAID
- C. Load balancing
- D. Virtualization

Answer: A

Explanation:

Anytime you connect multiple computers to work/act together as a single server, it is known as clustering. Clustered systems utilize parallel processing (improving performance and availability) and add redundancy (but also add costs).

QUESTION NO: 414

Which of the following technologies uses multiple devices to share work?

- A. Switching
- B. Load balancing
- C. RAID
- D. VPN concentrator

Answer: B

Explanation:

Load balancing is a way of providing high availability by splitting the workload across multiple computers.

QUESTION NO: 415

Which of the following provides the BEST application availability and is easily expanded as demand grows?

- A. Server virtualization
- B. Load balancing
- C. Active-Passive Cluster
- D. RAID 6

Answer: B

Explanation:

Load balancing is a way of providing high availability by splitting the workload across multiple computers.

QUESTION NO: 416

Which of the following can be utilized in order to provide temporary IT support during a disaster, where the organization sets aside funds for contingencies, but does not necessarily have a dedicated site to restore those services?

- A. Hot site
- B. Warm site
- C. Cold site
- D. Mobile site

Answer: D

Explanation:

Not having a dedicated site means that the mobile site can fill the role of either being a hot, warm or cold site as a disaster recovery measure.

QUESTION NO: 417

A security administrator has just finished creating a hot site for the company. This implementation relates to which of the following concepts?

- A. Confidentiality
- B. Availability
- C. Succession planning
- D. Integrity

Answer: B

Explanation:

Simply making sure that the data and systems are available for authorized users is what availability is all about. Data backups, redundant systems, and disaster recovery plans all support availability. And creating a hot site is about providing availability.

QUESTION NO: 418

Which of the following disaster recovery strategies has the highest cost and shortest recovery time?

- A. Warm site
- B. Hot site
- C. Cold site
- D. Co-location site

Answer: B

Explanation:

A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization. Databases can be kept up-to-date using network connections. These types of facilities are expensive, and they're primarily suitable for short-term situations.

QUESTION NO: 419

A company wants to ensure that its hot site is prepared and functioning. Which of the following would be the BEST process to verify the backup datacenter is prepared for such a scenario?

- A. Site visit to the backup data center
- B. Disaster recovery plan review
- C. Disaster recovery exercise
- D. Restore from backup

Answer: C

Explanation:

A hot site is a location that can provide operations within hours of a failure. This type of site would have servers, networks, and telecommunications equipment in place to reestablish service in a short time. Hot sites provide network connectivity, systems, and preconfigured software to meet the needs of an organization. This means that an actual exercise run would test the abilities of your hot site best.

QUESTION NO: 420

The Chief Information Officer (CIO) wants to implement a redundant server location to which the production server images can be moved within 48 hours and services can be quickly restored, in case of a catastrophic failure of the primary datacenter's HVAC. Which of the following can be implemented?

- A. Cold site
- B. Load balancing
- C. Warm site
- D. Hot site

Answer: C

Explanation:

Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement.

QUESTION NO: 421

Which of the following is the BEST concept to maintain required but non-critical server availability?

- A. SaaS site
- B. Cold site
- C. Hot site
- D. Warm site

Answer: D

Explanation:

Warm sites provide computer systems and compatible media capabilities. If a warm site is used, administrators and other staff will need to install and configure systems to resume operations. For

most organizations, a warm site could be a remote office, a leased facility, or another organization with which yours has a reciprocal agreement. Another term for a warm site/reciprocal site is active/active model.

QUESTION NO: 422

After copying a sensitive document from his desktop to a flash drive, Joe, a user, realizes that the document is no longer encrypted. Which of the following can a security technician implement to ensure that documents stored on Joe's desktop remain encrypted when moved to external media or other network based storage?

- A. Whole disk encryption
- B. Removable disk encryption
- C. Database record level encryption
- D. File level encryption

Answer: D

Explanation:

Encryption is used to ensure the confidentiality of information. In this case you should make use of file level encryption. File level encryption is a form of disk encryption where individual files or directories are encrypted by the file system itself. This is in contrast to full disk encryption where the entire partition or disk, in which the file system resides, is encrypted.

QUESTION NO: 423

Customers' credit card information was stolen from a popular video streaming company. A security consultant determined that the information was stolen, while in transit, from the gaming consoles of a particular vendor. Which of the following methods should the company consider to secure this data in the future?

- A. Application firewalls
- B. Manual updates
- C. Firmware version control
- D. Encrypted TCP wrappers

Answer: D

Explanation:

Wrapping sensitive systems with a specific control is required when protecting data in transit. TCP wrappers are also security controls. TCP Wrapper is a host-based networking ACL system, used to filter network access to Internet Protocol servers on (Unix-like) operating systems such as Linux

or BSD. It allows host or subnetwork IP addresses, names and/or inetd query replies, to be used as tokens on which to filter for access control purposes.

TCP Wrapper should not be considered a replacement for a properly configured firewall. Instead, TCP Wrapper should be used in conjunction with a firewall and other security enhancements in order to provide another layer of protection in the implementation of a security policy.

QUESTION NO: 424

Which of the following controls can be used to prevent the disclosure of sensitive information stored on a mobile device's removable media in the event that the device is lost or stolen?

- A. Hashing
- B. Screen locks
- C. Device password
- D. Encryption

Answer: D

Explanation:

Encryption is used to ensure the confidentiality of information.

QUESTION NO: 425

An online store wants to protect user credentials and credit card information so that customers can store their credit card information and use their card for multiple separate transactions.

Which of the following database designs provides the BEST security for the online store?

- A. Use encryption for the credential fields and hash the credit card field
- B. Encrypt the username and hash the password
- C. Hash the credential fields and use encryption for the credit card field
- D. Hash both the credential fields and the credit card field

Answer: C

Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables. One main characteristic of hashing is that the algorithm must have few or no collisions – in hashing two different inputs does not give the same output. Thus the credential fields should be hashed because anyone customer will have a unique credit card number/identity and since they will use their credit cards for many different transactions, the credit card field should be encrypted

only, not hashed.

QUESTION NO: 426

A system administrator has been instructed by the head of security to protect their data at-rest.

Which of the following would provide the strongest protection?

- A. Prohibiting removable media
- B. Incorporating a full-disk encryption system
- C. Biometric controls on data center entry points
- D. A host-based intrusion detection system

Answer: B

Explanation:

Full disk encryption can be used to encrypt an entire volume with 128-bit encryption. When the entire volume is encrypted, the data is not accessible to someone who might boot another operating system in an attempt to bypass the computer's security. Full disk encryption is sometimes referred to as hard drive encryption. This would be best to protect data that is at rest.

QUESTION NO: 427

Several departments within a company have a business need to send high volumes of confidential information to customers via email. Which of the following is the BEST solution to mitigate unintentional exposure of confidential information?

- A. Employ encryption on all outbound emails containing confidential information.
- B. Employ exact data matching and prevent inbound emails with Data Loss Prevention.
- C. Employ hashing on all outbound emails containing confidential information.
- D. Employ exact data matching and encrypt inbound e-mails with Data Loss Prevention.

Answer: A

Explanation:

Encryption is used to ensure the confidentiality of information and in this case the outbound email that contains the confidential information should be encrypted.

QUESTION NO: 428

After recovering from a data breach in which customer data was lost, the legal team meets with

the Chief Security Officer (CSO) to discuss ways to better protect the privacy of customer data.

Which of the following controls support this goal?

- A. Contingency planning
- B. Encryption and stronger access control
- C. Hashing and non-repudiation
- D. Redundancy and fault tolerance

Answer: B

Explanation:

Encryption is used to protect data/contents/documents. Access control refers to controlling who accesses any data/contents/documents and to exercise authorized control to the accessing of that data.

QUESTION NO: 429

A security audit identifies a number of large email messages being sent by a specific user from their company email account to another address external to the company. These messages were sent prior to a company data breach, which prompted the security audit. The user was one of a few people who had access to the leaked data. Review of the suspect's emails show they consist mostly of pictures of the user at various locations during a recent vacation. No suspicious activities from other users who have access to the data were discovered.

Which of the following is occurring?

- A. The user is encrypting the data in the outgoing messages.
- B. The user is using steganography.
- C. The user is spamming to obfuscate the activity.
- D. The user is using hashing to embed data in the emails.

Answer: B

Explanation:

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

QUESTION NO: 430

A security analyst has been notified that trade secrets are being leaked from one of the executives in the corporation. When reviewing this executive's laptop they notice several pictures of the employee's pets are on the hard drive and on a cloud storage network. When the analyst hashes the images on the hard drive against the hashes on the cloud network they do not match.

Which of the following describes how the employee is leaking these secrets?

- A. Social engineering
- B. Steganography
- C. Hashing
- D. Digital signatures

Answer: B

Explanation:

Steganography is the process of hiding one message in another. Steganography may also be referred to as electronic watermarking. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

QUESTION NO: 431

Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

- A. Hashing
- B. Stream ciphers
- C. Steganography
- D. Block ciphers

Answer: A

Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables one of its characteristics is that it must be one-way – it is not reversible.

QUESTION NO: 432

A software developer wants to prevent stored passwords from being easily decrypted. When the

password is stored by the application, additional text is added to each password before the password is hashed. This technique is known as:

- A. Symmetric cryptography.
- B. Private key cryptography.
- C. Salting.
- D. Rainbow tables.

Answer: C

Explanation:

Salting can be used to strengthen the hashing when the passwords were encrypted. Though hashing is a one-way algorithm it does not mean that it cannot be hacked. One method to hack a hash is through rainbow tables and salt is the counter measure to rainbow tables. With salt a password that you typed in and that has been encrypted with a hash will yield a letter combination other than what you actually types in when it is rainbow table attacked.

QUESTION NO: 433

Which of the following concepts describes the use of a one way transformation in order to validate the integrity of a program?

- A. Hashing
- B. Key escrow
- C. Non-repudiation
- D. Steganography

Answer: A

Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and its main characteristics are:

It must be one-way – it is not reversible.

Variable-length input produces fixed-length output – whether you have two characters or 2 million, the hash size is the same.

The algorithm must have few or no collisions – in hashing two different inputs does not give the same output.

QUESTION NO: 434

The security administrator is implementing a malware storage system to archive all malware seen

by the company into a central database. The malware must be categorized and stored based on similarities in the code. Which of the following should the security administrator use to identify similar malware?

- A. TwoFish
- B. SHA-512
- C. Fuzzy hashes
- D. HMAC

Answer: C

Explanation:

Hashing is used to ensure that a message has not been altered. It can be useful for positively identifying malware when a suspected file has the same hash value as a known piece of malware. However, modifying a single bit of a malicious file will alter its hash value. To counter this, a continuous stream of hash values is generated for rolling block of code. This can be used to determine the similarity between a suspected file and known pieces of malware.

QUESTION NO: 435

An Information Systems Security Officer (ISSO) has been placed in charge of a classified peer-to-peer network that cannot connect to the Internet. The ISSO can update the antivirus definitions manually, but which of the following steps is MOST important?

- A. A full scan must be run on the network after the DAT file is installed.
- B. The signatures must have a hash value equal to what is displayed on the vendor site.
- C. The definition file must be updated within seven days.
- D. All users must be logged off of the network prior to the installation of the definition file.

Answer: B

Explanation:

A hash value can be used to uniquely identify secret information. This requires that the hash function is collision resistant, which means that it is very hard to find data that generate the same hash value and thus it means that in hashing two different inputs will not yield the same output. Thus the hash value must be equal to that displayed on the vendor site.

QUESTION NO: 436

Which of the following would a security administrator use to verify the integrity of a file?

- A. Time stamp
- B. MAC times
- C. File descriptor
- D. Hash

Answer: D

Explanation:

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables and it is a one-way transformation in order to validate the integrity of data.

QUESTION NO: 437

Sara, a security administrator, manually hashes all network device configuration files daily and compares them to the previous days' hashes. Which of the following security concepts is Sara using?

- A. Confidentiality
- B. Compliance
- C. Integrity
- D. Availability

Answer: C

Explanation:

Integrity means the message can't be altered without detection.

QUESTION NO: 438

Matt, a forensic analyst, wants to obtain the digital fingerprint for a given message. The message is 160-bits long. Which of the following hashing methods would Matt have to use to obtain this digital fingerprint?

- A. SHA1
- B. MD2
- C. MD4
- D. MD5

Answer: A

Explanation:

The Secure Hash Algorithm (SHA) was designed to ensure the integrity of a message. SHA is a one-way hash that provides a hash value that can be used with an encryption protocol. This

algorithm produces a 160-bit hash value. SHA (1 or 2) is preferred over Message Digest Algorithm.

QUESTION NO: 439

Company A submitted a bid on a contract to do work for Company B via email. Company B was insistent that the bid did not come from Company A. Which of the following would have assured that the bid was submitted by Company A?

- A. Steganography
- B. Hashing
- C. Encryption
- D. Digital Signatures

Answer: D

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

QUESTION NO: 440

An email client says a digital signature is invalid and the sender cannot be verified. The recipient is concerned with which of the following concepts?

- A. Integrity
- B. Availability
- C. Confidentiality
- D. Remediation

Answer: A

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message. Digital Signatures is used to validate the integrity of the message and the sender. Integrity means the message can't be altered without detection.

QUESTION NO: 441

A software firm posts patches and updates to a publicly accessible FTP site. The software firm also posts digitally signed checksums of all patches and updates. The firm does this to address:

- A. Integrity of downloaded software.
- B. Availability of the FTP site.
- C. Confidentiality of downloaded software.
- D. Integrity of the server logs.

Answer: A

Explanation:

Digital Signatures is used to validate the integrity of the message and the sender. In this case the software firm that posted the patches and updates digitally signed the checksums of all patches and updates.

QUESTION NO: 442

It is important to staff who use email messaging to provide PII to others on a regular basis to have confidence that their messages are not intercepted or altered during transmission. They are concerned about which of the following types of security control?

- A. Integrity
- B. Safety
- C. Availability
- D. Confidentiality

Answer: A

Explanation:

Integrity means that the messages/ data is not altered. PII is personally identifiable information that can be used to uniquely identify an individual. PII can be used to ensure the integrity of data/messages.

QUESTION NO: 443

Matt, a security administrator, wants to ensure that the message he is sending does not get intercepted or modified in transit. This concern relates to which of the following concepts?

- A. Availability
- B. Integrity

- C. Accounting
- D. Confidentiality

Answer: B

Explanation:

Integrity means ensuring that data has not been altered. Hashing and message authentication codes are the most common methods to accomplish this. In addition, ensuring nonrepudiation via digital signatures supports integrity.

QUESTION NO: 444

Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?

- A. Recipient's private key
- B. Sender's public key
- C. Recipient's public key
- D. Sender's private key

Answer: B

Explanation:

When the sender wants to send a message to the receiver. It's important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus the recipient uses the sender's public key to verify the sender's identity.

QUESTION NO: 445

Digital signatures are used for ensuring which of the following items? (Select TWO).

- A. Confidentiality
- B. Integrity
- C. Non-Repudiation
- D. Availability
- E. Algorithm strength

Answer: B,C

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. The message is encrypted using the encryption system, and a second piece of information, the digital signature, is added to the message.

Nonrepudiation prevents one party from denying actions that they carried out and in the electronic world nonrepudiation measures can be a two-key cryptographic system and the involvement of a third party to verify the validity. This respected third party 'vouches' for the individuals in the two-key system. Thus non-repudiation also impacts on integrity.

QUESTION NO: 446

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify that the email came from Joe and decrypt it? (Select TWO).

- A. The CA's public key
- B. Ann's public key
- C. Joe's private key
- D. Ann's private key
- E. The CA's private key
- F. Joe's public key

Answer: D,F

Explanation:

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe—the public key—to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be.

QUESTION NO: 447

Joe, a user, wants to send an encrypted email to Ann. Which of the following will Ann need to use to verify the validity's of Joe's certificate? (Select TWO).

- A. The CA's public key

- B. Joe's private key
- C. Ann's public key
- D. The CA's private key
- E. Joe's public key
- F. Ann's private key

Answer: A,E

Explanation:

Joe wants to send a message to Ann. It's important that this message not be altered. Joe will use the private key to create a digital signature. The message is, in effect, signed with the private key. Joe then sends the message to Ann. Ann will use the public key attached to the message to validate the digital signature. If the values match, Ann knows the message is authentic and came from Joe. Ann will use a key provided by Joe—the public key—to decrypt the message. Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit. Thus Ann would compare the signature area referred to as a message in the message with the calculated value digest (her private key in this case). If the values match, the message hasn't been tampered with and the originator is verified as the person they claim to be. This process provides message integrity, nonrepudiation, and authentication. A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. A certificate is nothing more than a mechanism that associates the public key with an individual.

If Joe wants to send Ann an encrypted e-mail, there should be a mechanism to verify to Ann that the message received from Mike is really from Joe. If a third party (the CA) vouches for Joe and Ann trusts that third party, Ann can assume that the message is authentic because the third party says so.

QUESTION NO: 448

A user was reissued a smart card after the previous smart card had expired. The user is able to log into the domain but is now unable to send digitally signed or encrypted email. Which of the following would the user need to perform?

- A. Remove all previous smart card certificates from the local certificate store.
- B. Publish the new certificates to the global address list.
- C. Make the certificates available to the operating system.
- D. Recover the previous smart card certificates.

Answer: B

Explanation:

CAs can be either private or public, with VeriSign being one of the best known of the public variety. Many operating system providers allow their systems to be configured as CA systems.

These CA systems can be used to generate internal certificates that are used within a business or in large external settings. The process provides certificates to the users. Since the user in question has been re-issued a smart card, the user must receive a new certificate by the CA to allow the user to send digitally signed email. This is achieved by publishing the new certificates to the global address list.

QUESTION NO: 449

Which of the following could cause a browser to display the message below?

"The security certificate presented by this website was issued for a different website's address."

- A. The website certificate was issued by a different CA than what the browser recognizes in its trusted CAs.
- B. The website is using a wildcard certificate issued for the company's domain.
- C. HTTPS://127.0.0.1 was used instead of HTTPS://localhost.
- D. The website is using an expired self signed certificate.

Answer: C

Explanation:

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. In typical public key infrastructure (PKI) arrangements, a digital signature from a certificate authority (CA) attests that a particular public key certificate is valid (i.e., contains correct information). Users, or their software on their behalf, check that the private key used to sign some certificate matches the public key in the CA's certificate. Since CA certificates are often signed by other, "higher-ranking," CAs, there must necessarily be a highest CA, which provides the ultimate in attestation authority in that particular PKI scheme.

Localhost is a hostname that means this computer and may be used to access the computer's own network services via its loopback network interface. Using the loopback interface bypasses local network interface hardware. In this case the HTTPS://127.0.0.1 was used and not HTTPS://localhost

QUESTION NO: 450

Certificates are used for: (Select TWO).

- A. Client authentication.
- B. WEP encryption.

- C. Access control lists.
- D. Code signing.
- E. Password hashing.

Answer: A,D

Explanation:

Certificates are used in PKI to digitally sign data, information, files, email, code, etc. Certificates are also used in PKI for client authentication.

QUESTION NO: 451

Some customers have reported receiving an untrusted certificate warning when visiting the company's website. The administrator ensures that the certificate is not expired and that customers have trusted the original issuer of the certificate. Which of the following could be causing the problem?

- A. The intermediate CA certificates were not installed on the server.
- B. The certificate is not the correct type for a virtual server.
- C. The encryption key used in the certificate is too short.
- D. The client's browser is trying to negotiate SSL instead of TLS.

Answer: A

Explanation:

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't.

QUESTION NO: 452

Digital certificates can be used to ensure which of the following? (Select TWO).

- A. Availability
- B. Confidentiality
- C. Verification
- D. Authorization
- E. Non-repudiation

Answer: B,E

Explanation:

Digital Signatures is used to validate the integrity of the message and the sender. Digital certificates refer to cryptography which is mainly concerned with Confidentiality, Integrity, Authentication, Nonrepudiation and Access Control. Nonrepudiation prevents one party from denying actions they carried out.

QUESTION NO: 453

A certificate used on an ecommerce web server is about to expire. Which of the following will occur if the certificate is allowed to expire?

- A. The certificate will be added to the Certificate Revocation List (CRL).
- B. Clients will be notified that the certificate is invalid.
- C. The ecommerce site will not function until the certificate is renewed.
- D. The ecommerce site will no longer use encryption.

Answer: B

Explanation:

A similar process to certificate revocation will occur when a certificate is allowed to expire. Notification will be sent out to clients of the invalid certificate. The process of revoking a certificate begins when the CA is notified that a particular certificate needs to be revoked. This must be done whenever the private key becomes known. The owner of a certificate can request that it be revoked at any time, or the administrator can make the request.

QUESTION NO: 454

An administrator has successfully implemented SSL on srv4.comptia.com using wildcard certificate *.comptia.com, and now wishes to implement SSL on srv5.comptia.com. Which of the following files should be copied from srv4 to accomplish this?

- A. certificate, private key, and intermediate certificate chain
- B. certificate, intermediate certificate chain, and root certificate
- C. certificate, root certificate, and certificate signing request
- D. certificate, public key, and certificate signing request

Answer: A

Explanation:

a wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. In public-key cryptography, the receiver has a private key known only to them; a public key corresponds to it, which they make known to others. The public key can be sent to all other

parties; the private key is never divulged. A symmetric algorithm requires that receivers of the message use the same private key. Thus you should copy the certificate, the private key and the intermediate certificate chain from srv4 to srv5.

QUESTION NO: 455

An encrypted message is sent using PKI from Sara, a client, to a customer. Sara claims she never sent the message. Which of the following aspects of PKI BEST ensures the identity of the sender?

- A. CRL
- B. Non-repudiation
- C. Trust models
- D. Recovery agents

Answer: B

Explanation:

Nonrepudiation prevents one party from denying actions they carried out. This means that the identity of the email sender will not be repudiated.

QUESTION NO: 456

Ann, a newly hired human resource employee, sent out confidential emails with digital signatures, to an unintended group. Which of the following would prevent her from denying accountability?

- A. Email Encryption
- B. Steganography
- C. Non Repudiation
- D. Access Control

Answer: C

Explanation:

Nonrepudiation prevents one party from denying actions they carried out.

QUESTION NO: 457

A company recently experienced data loss when a server crashed due to a midday power outage. Which of the following should be used to prevent this from occurring again?

- A. Recovery procedures
- B. EMI shielding
- C. Environmental monitoring
- D. Redundancy

Answer: D

Explanation:

Redundancy refers to systems that either are duplicated or fail over to other systems in the event of a malfunction (in this case a power outage). Failover refers to the process of reconstructing a system or switching over to other systems when a failure is detected. In the case of a server, the server switches to a redundant server when a fault is detected. This strategy allows service to continue uninterrupted until the primary server can be restored.

QUESTION NO: 458

Matt, a security consultant, has been tasked with increasing server fault tolerance and has been given no budget to accomplish his task. Which of the following can Matt implement to ensure servers will withstand hardware failure?

- A. Hardware load balancing
- B. RAID
- C. A cold site
- D. A host standby

Answer: B

Explanation:

Fault tolerance is the ability of a system to sustain operations in the event of a component failure. Fault-tolerant systems can continue operation even though a critical component, such as a disk drive, has failed. This capability involves overengineering systems by adding redundant components and subsystems. RAID can achieve fault tolerance using software which can be done using the existing hardware and software.

QUESTION NO: 459

After a company has standardized to a single operating system, not all servers are immune to a well-known OS vulnerability. Which of the following solutions would mitigate this issue?

- A. Host based firewall
- B. Initial baseline configurations
- C. Discretionary access control

D. Patch management system

Answer: D

Explanation:

A patch is an update to a system. Sometimes a patch adds new functionality; in other cases, it corrects a bug in the software. Patch Management can thus be used to fix security problems discovered within the OS thus negating a known OS vulnerability.

QUESTION NO: 460

A security manager requires fencing around the perimeter, and cipher locks on all entrances. The manager is concerned with which of the following security controls?

- A. Integrity**
- B. Availability**
- C. Confidentiality**
- D. Safety**

Answer: D

Explanation:

Fencing is used to increase physical security and safety. Locks are used to keep those who are unauthorized out.

QUESTION NO: 461

A cafe provides laptops for Internet access to their customers. The cafe is located in the center corridor of a busy shopping mall. The company has experienced several laptop thefts from the cafe during peak shopping hours of the day. Corporate has asked that the IT department provide a solution to eliminate laptop theft. Which of the following would provide the IT department with the BEST solution?

- A. Attach cable locks to each laptop**
- B. Require each customer to sign an AUP**
- C. Install a GPS tracking device onto each laptop**
- D. Install security cameras within the perimeter of the café**

Answer: A

Explanation:

All laptop cases include a built-in security slot in which a cable lock can be inserted to prevent it from easily being removed from the premises.

QUESTION NO: 462

A business has set up a Customer Service kiosk within a shopping mall. The location will be staffed by an employee using a laptop during the mall business hours, but there are still concerns regarding the physical safety of the equipment while it is not in use. Which of the following controls would BEST address this security concern?

- A. Host-based firewall
- B. Cable locks
- C. Locking cabinets
- D. Surveillance video

Answer: C

Explanation:

Locking cabinets can be used to protect backup media, documentation and other physical artefacts. In this case a locking cabinet will keep the company's Customer Service kiosk under lock and key when not in use.

QUESTION NO: 463

Although a vulnerability scan report shows no vulnerabilities have been discovered, a subsequent penetration test reveals vulnerabilities on the network. Which of the following has been reported by the vulnerability scan?

- A. Passive scan
- B. Active scan
- C. False positive
- D. False negative

Answer: D

Explanation:

With a false negative, you are not alerted to a situation when you should be alerted. A False negative is exactly the opposite of a false positive.

QUESTION NO: 464

Which of the following documents outlines the technical and security requirements of an

agreement between organizations?

- A. BPA
- B. RFQ
- C. ISA
- D. RFC

Answer: C

Explanation:

ISA/ Interconnection Security Agreement is an agreement between two organizations that have connected systems. The agreement documents the technical requirements of the connected systems.

QUESTION NO: 465

A large bank has moved back office operations offshore to another country with lower wage costs in an attempt to improve profit and productivity. Which of the following would be a customer concern if the offshore staff had direct access to their data?

- A. Service level agreements
- B. Interoperability agreements
- C. Privacy considerations
- D. Data ownership

Answer: C

Explanation:

Businesses such as banks have legally mandated privacy requirements and with moving operations offshore there is decentralized control with has implications for privacy of data.

QUESTION NO: 466

Which of the following are examples of detective controls?

- A. Biometrics, motion sensors and mantraps.
- B. Audit, firewall, anti-virus and biometrics.
- C. Motion sensors, intruder alarm and audit.
- D. Intruder alarm, mantraps and firewall.

Answer: C

Explanation:

Detective controls are those that operate afterward so as to discover that has happened. Detective controls include security guards, motion detectors, recording and reviewing of events captured by security cameras or CCTV, job rotation, mandatory vacations, audit trails, honeypots or honeynets, IDSs, violation reports, supervision and reviews of users, and incident investigations.

QUESTION NO: 467

An organization processes credit card transactions and is concerned that an employee may intentionally email credit card numbers to external email addresses. This company should consider which of the following technologies?

- A. IDS
- B. Firewalls
- C. DLP
- D. IPS

Answer: C

Explanation:

A Data Loss Prevention technology is aimed at detecting and preventing unauthorized access to, use of, or transmission of sensitive information such as credit card details.

QUESTION NO: 468

Which of the following, if properly implemented, would prevent users from accessing files that are unrelated to their job duties? (Select TWO).

- A. Separation of duties
- B. Job rotation
- C. Mandatory vacation
- D. Time of day restrictions
- E. Least privilege

Answer: A,E

Explanation:

Separation of duties means that users are granted only the permissions they need to do their work and no more. More so it means that you are employing best practices. The segregation of duties and separation of environments is a way to reduce the likelihood of misuse of systems or information. A separation of duties policy is designed to reduce the risk of fraud and to prevent other losses in an organization.

A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

QUESTION NO: 469

Which of the following helps to establish an accurate timeline for a network intrusion?

- A. Hashing images of compromised systems
- B. Reviewing the date of the antivirus definition files
- C. Analyzing network traffic and device logs
- D. Enforcing DLP controls at the perimeter

Answer: C

Explanation:

Network activity as well as intrusion can be viewed on device logs and by analyzing the network traffic that passed through your network. Thus to establish an accurate timeline for a network intrusion you can look at and analyze the device logs and network traffic to yield the appropriate information.

QUESTION NO: 470

A recent audit has revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

- A. Deploy a honeypot
- B. Disable unnecessary services
- C. Change default passwords
- D. Implement an application firewall
- E. Penetration testing

Answer: B,C

Explanation:

Increasing security posture is akin to getting the appropriate type of risk mitigation for your company. A plan and its implementation is a major part of security posture. When new servers and network devices are being deployed your most vulnerable points will be coming from all unnecessary services that may be running from servers and network default passwords. Thus your plan should be to disable those services that are not needed and change the default password during the deployment of the new servers and network devices.

QUESTION NO: 471

Joe is the accounts payable agent for ABC Company. Joe has been performing accounts payable function for the ABC Company without any supervision. Management has noticed several new accounts without billing invoices that were paid. Which of the following is the BEST management option for review of the new accounts?

- A. Mandatory vacation
- B. Job rotation
- C. Separation of duties
- D. Replacement

Answer: A

Explanation:

A mandatory vacation policy requires all users to take time away from work to refresh. Mandatory vacation give the employee a chance to refresh, but it also gives the company a chance to make sure that others can fill in any gaps in skills and satisfies the need to have replication or duplication at all levels. Mandatory vacations also provide an opportunity to discover fraud. In this case mandatory vacations can allow the company to review all the new accounts.

QUESTION NO: 472

A company hosts its public websites internally. The administrator would like to make some changes to the architecture.

The three goals are:

reduce the number of public IP addresses in use by the web servers

drive all the web traffic through a central point of control

mitigate automated attacks that are based on IP address scanning

Which of the following would meet all three goals?

- A. Firewall
- B. Load balancer
- C. URL filter
- D. Reverse proxy

Answer: D

Explanation:

The purpose of a proxy server is to serve as a proxy or middle man between clients and servers. Using a reverse proxy you will be able to meet the three stated goals.

QUESTION NO: 473

The IT department noticed that there was a significant decrease in network performance during the afternoon hours. The IT department performed analysis of the network and discovered this was due to users accessing and downloading music and video streaming from social sites. The IT department notified corporate of their findings and a memo was sent to all employees addressing the misuse of company resources and requesting adherence to company policy. Which of the following policies is being enforced?

- A. Acceptable use policy
- B. Telecommuting policy
- C. Data ownership policy
- D. Non disclosure policy

Answer: A

Explanation:

Acceptable use policy describes how employees are allowed to use company systems and resources, and the consequences of misuse.

QUESTION NO: 474

A computer security officer has investigated a possible data breach and has found it credible. The officer notifies the data center manager and the Chief Information Security Officer (CISO). This is an example of:

- A. escalation and notification.
- B. first responder.
- C. incident identification.
- D. incident mitigation.

Answer: A

Explanation:

Escalation and notification is a response strategy that outlines a staged procedure of escalation and notification that is to be followed in the event of a security incident. Only those in specific positions of authority or responsibility must receive notification of the security breach.

QUESTION NO: 475

A company would like to take electronic orders from a partner; however, they are concerned that a non-authorized person may send an order. The legal department asks if there is a solution that provides non-repudiation. Which of the following would meet the requirements of this scenario?

- A. Encryption
- B. Digital signatures
- C. Steganography
- D. Hashing
- E. Perfect forward secrecy

Answer: B

Explanation:

A digital signature is an electronic mechanism to prove that a message was sent from a specific user (that is, it provides for non-repudiation) and that the message wasn't changed while in transit (it also provides integrity). Thus digital signatures will meet the stated requirements.

QUESTION NO: 476

The Chief Security Officer (CSO) is contacted by a first responder. The CSO assigns a handler. Which of the following is occurring?

- A. Unannounced audit response
- B. Incident response process
- C. Business continuity planning
- D. Unified threat management
- E. Disaster recovery process

Answer: B

Explanation:

The Incident response policy outlines the processes that should be followed when an incident occurs. Thus when a CSO is contacted by a first responder and then assign a handler for the incident it is clearly the incident response process that is put in practice.

QUESTION NO: 477

A security administrator is auditing a database server to ensure the correct security measures are

in place to protect the data. Some of the fields consist of people's first name, last name, home address, date of birth and mothers last name. Which of the following describes this type of data?

- A. PII
- B. PCI
- C. Low
- D. Public

Answer: A

Explanation:

PII is any type of information/data and portion of data that can be used to trace back to a person and is usually data like personally identifiable information such as first names, last names, home address, date of birth, etc.

QUESTION NO: 478

Several employees clicked on a link in a malicious message that bypassed the spam filter and their PCs were infected with malware as a result. Which of the following BEST prevents this situation from occurring in the future?

- A. Data loss prevention
- B. Enforcing complex passwords
- C. Security awareness training
- D. Digital signatures

Answer: C

Explanation:

Security awareness and training include explaining policies, procedures, and current threats to both users and management. A security awareness and training program can do much to assist in your efforts to improve and maintain security. Ideally, a security awareness training program for the entire organization should cover the following areas:

Importance of security

Responsibilities of people in the organization

Policies and procedures

Usage policies

Account and password-selection criteria

Social engineering prevention

QUESTION NO: 479

Visible security cameras are considered to be which of the following types of security controls?

- A. Technical
- B. Compensating
- C. Deterrent
- D. Administrative

Answer: C

Explanation:

Since a deterrent access control method is designed to discourage the violation of security policies, so a camera can be used to discourage individuals from taking unwanted action.

QUESTION NO: 480

A security administrator would like to ensure that system administrators are not using the same password for both their privileged and non-privileged accounts. Which of the following security controls BEST accomplishes this goal?

- A. Require different account passwords through a policy
- B. Require shorter password expiration for non-privileged accounts
- C. Require shorter password expiration for privileged accounts
- D. Require a greater password length for privileged accounts

Answer: A

Explanation:

A password policy aka account policy enforcement can be configured in such a way so as to make sure that system administrators make use of different passwords for different accounts.

QUESTION NO: 481

Ann, a security analyst, has discovered that her company has very high staff turnover and often user accounts are not disabled after an employee leaves the company. Which of the following could Ann implement to help identify accounts that are still active for terminated employees?

- A. Routine audits
- B. Account expirations
- C. Risk assessments
- D. Change management

Answer: A

Explanation:

Routine audits are carried out after you have implemented security controls based on risk. These audits include aspects such as user rights and permissions and specific events.

QUESTION NO: 482

Ann, the system administrator, is installing an extremely critical system that can support ZERO downtime. Which of the following BEST describes the type of system Ann is installing?

- A. High availability
- B. Clustered
- C. RAID
- D. Load balanced

Answer: A

Explanation:

High Availability is the term used to refer to a system that has been secured and set up/configured in such a way so as to be online, active and able to respond and thus have zero downtime as a result.

QUESTION NO: 483

A systems engineer has been presented with storage performance and redundancy requirements for a new system to be built for the company. The storage solution must be designed to support the highest performance and must also be able to support more than one drive failure. Which of the following should the engineer choose to meet these requirements?

- A. A mirrored striped array with parity
- B. A mirrored mirror array
- C. A striped array
- D. A striped array with parity

Answer: B

Explanation:

Mirroring means the data written to one drive is exactly duplicated to a second drive in real time. Disk mirroring is also known as RAID 1 and the data is intact in a RAID 1 array if either one of the two drives fails. After the failed drive is replaced with a new drive, you remirror the data from the good drive to the new drive to re-create the array.

QUESTION NO: 484

In order to secure additional budget, a security manager wants to quantify the financial impact of a one-time compromise. Which of the following is MOST important to the security manager?

- A. Impact
- B. SLE
- C. ALE
- D. ARO

Answer: B

Explanation:

SLE is a monetary value, and it represents how much you expect to lose at any one time: the single loss expectancy. SLE can be divided into two components: AV (asset value) and the EF (exposure factor). Thus a one-time compromise would resort under the SLE for the security manager.

QUESTION NO: 485

A company has just deployed a centralized event log storage system. Which of the following can be used to ensure the integrity of the logs after they are collected?

- A. Write-once drives
- B. Database encryption
- C. Continuous monitoring
- D. Role-based access controls

Answer: A

Explanation:

A write-once drive means that the disk cannot be overwritten once data is written to the disk; and thus the integrity of the logs, if they are written to a write-once drives will ensure integrity of those logs.

QUESTION NO: 486

Several departments in a corporation have a critical need for routinely moving data from one system to another using removable storage devices. Senior management is concerned with data loss and the introduction of malware on the network. Which of the following choices BEST

mitigates the range of risks associated with the continued use of removable storage devices?

- A. Remote wiping enabled for all removable storage devices
- B. Full-disk encryption enabled for all removable storage devices
- C. A well defined acceptable use policy
- D. A policy which details controls on removable storage use

Answer: D

Explanation:

Removable storage is both a benefit and a risk and since not all mobile devices support removable storage, the company has to have a comprehensive policy which details the controls of the use of removable s to mitigate the range of risks that are associated with the use of these devices.

QUESTION NO: 487

A company executive's laptop was compromised, leading to a security breach. The laptop was placed into storage by a junior system administrator and was subsequently wiped and re-imaged. When it was determined that the authorities would need to be involved, there was little evidence to present to the investigators. Which of the following procedures could have been implemented to aid the authorities in their investigation?

- A. A comparison should have been created from the original system's file hashes
- B. Witness testimony should have been taken by the administrator
- C. The company should have established a chain of custody tracking the laptop
- D. A system image should have been created and stored

Answer: D

Explanation:

A system image is a snapshot of what it and if a system image of the compromised system was created and stored, it is a useful tool when the authorities want to revisit the issue to investigate the incident.

QUESTION NO: 488

A company has recently allowed employees to take advantage of BYOD by installing WAPs throughout the corporate office. An employee, Joe, has recently begun to view inappropriate material at work using his personal laptop. When confronted, Joe indicated that he was never told that he could not view that type of material on his personal laptop. Which of the following should the company have employees acknowledge before allowing them to access the corporate WLAN with their personal devices?

- A. Privacy Policy
- B. Security Policy
- C. Consent to Monitoring Policy
- D. Acceptable Use Policy

Answer: D

Explanation:

Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

QUESTION NO: 489

A company has two server administrators that work overnight to apply patches to minimize disruption to the company. With the limited working staff, a security engineer performs a risk assessment to ensure the protection controls are in place to monitor all assets including the administrators in case of an emergency. Which of the following should be in place?

- A. NIDS
- B. CCTV
- C. Firewall
- D. NIPS

Answer: B

Explanation:

CCTV are an excellent way to deter unwanted activity and it records the occurrence of the event, in case it does happen. Cameras can be placed to watch points of entry, to monitor activities around valuable assets as well as provide additional protection in areas such as parking areas and walkways.

QUESTION NO: 490

A company's Chief Information Officer realizes the company cannot continue to operate after a disaster. Which of the following describes the disaster?

- A. Risk
- B. Asset
- C. Threat
- D. Vulnerability

Answer: C

Explanation:

Threat is basically anything that can take advantage of any vulnerability that may be found. When the CIO realizes that the company cannot continue to operate after a disaster, the disaster is then the threat to the company.

QUESTION NO: 491

Ann, the Chief Technology Officer (CTO), has agreed to allow users to bring their own device (BYOD) in order to leverage mobile technology without providing every user with a company owned device. She is concerned that users may not understand the company's rules, and she wants to limit potential legal concerns. Which of the following is the CTO concerned with?

- A. Data ownership
- B. Device access control
- C. Support ownership
- D. Acceptable use

Answer: A

Explanation:

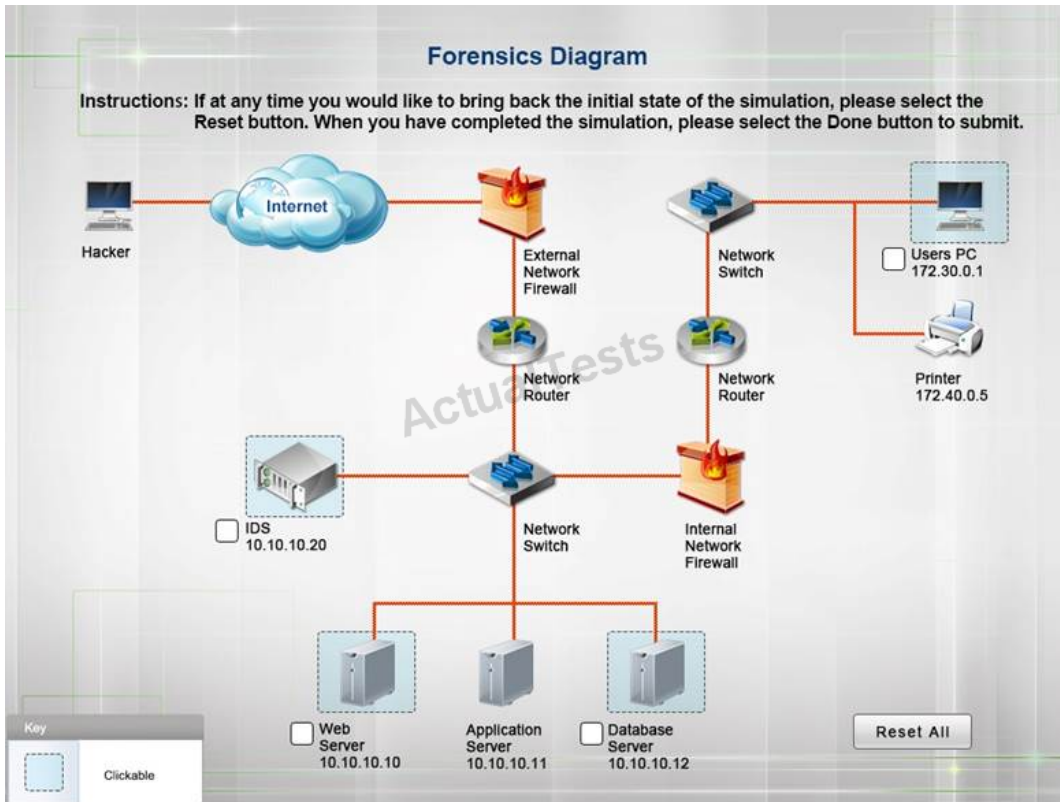
Issues of limiting potential legal concerns regarding company rules where users are allowed to bring their own devices is the premise of data ownership. When a third party (in this case the user's own device) is involved in a data exchange when clear rules and restrictions should be applied regarding data ownership.

QUESTION NO: 492 CORRECT TEXT

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incident responses.

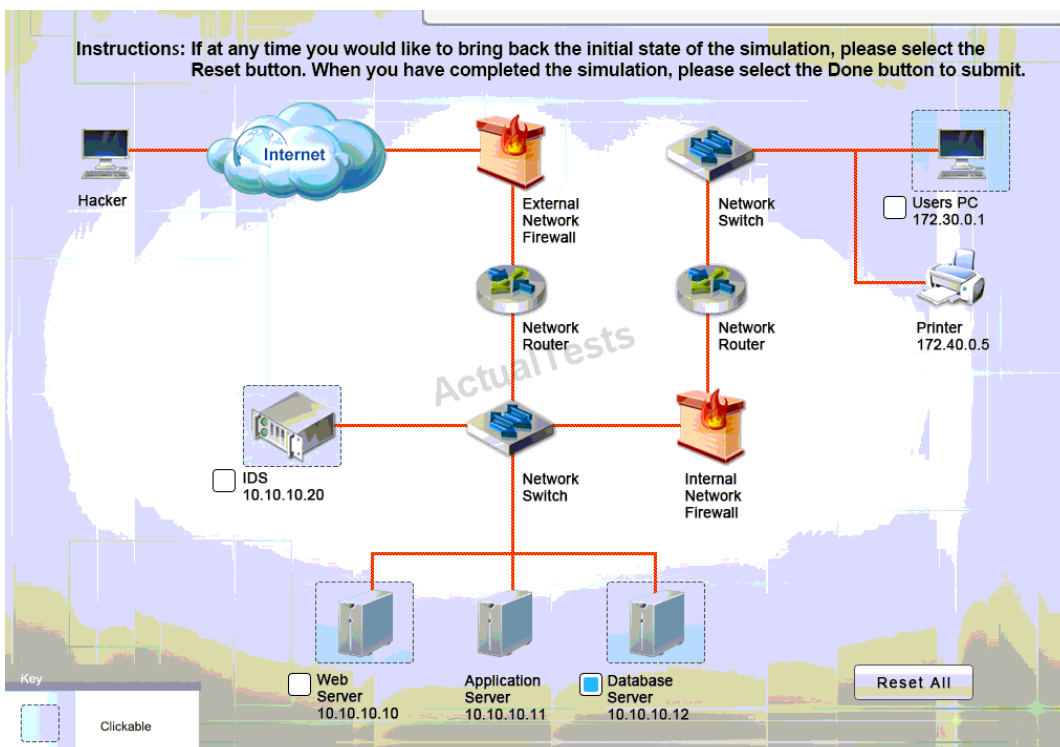
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at anytime you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Answer: Database server was attacked; actions should be to capture network traffic and Chain of Custody.

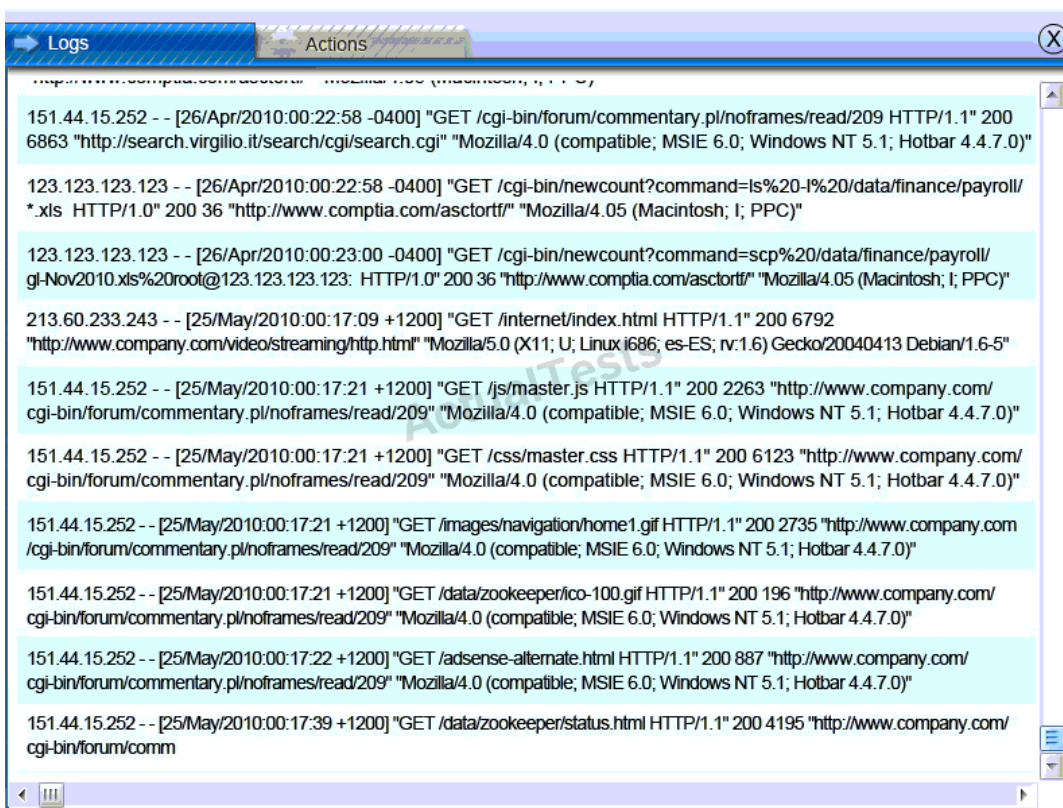
Explanation:

(The database server logs shows the Audit Failure and Audit Success attempts) It is only logical that all the logs will be stored on the database server and the least disruption action on the network to take as a response to the incident would be to check the logs (since these are already collected and stored) and maintain a chain of custody of those logs.



No.	Time	Source	Destination	Protocol	Length	Info
1	0	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
2	2.006303	Cisco_87:85:04	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/100/00:1c:0e:87:78:00 Cost = 4 Port = 0x8004
3	4.009585	172.31.146.123.2	172.31.146.123.1	ICMP	118	Echo (ping) request id=0x0001, seq=1/256, ttl=255
4	6.014086	172.31.146.123.1	172.31.146.123.2	ICMP	118	Echo (ping) reply id=0x0001, seq=1/256, ttl=255
5	7.911131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls HTTP/1.1
6	8.003312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
7	7.911131	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=whoami HTTP/1.1
8	8.003312	10.10.10.10	123.123.123.123	HTTP	260	HTTP/1.1 200 OK (text/html)
9	10.1232	123.123.123.123	10.10.10.10	HTTP	488	GET /cgi-bin/newcount?command=ls%20%20(%2fetc/passwd)/* via HTTP/1.1

246



Database Server Log:

Topic 3, Threats and Vulnerabilities

QUESTION NO: 493

Which of the following malware types may require user interaction, does not hide itself, and is commonly identified by marketing pop-ups based on browsing habits?

- A. Botnet
- B. Rootkit
- C. Adware
- D. Virus

Answer: C

Explanation:

Adware is free software that is supported by advertisements. Common adware programs are toolbars, games and utilities. They are free to use, but require you to watch advertisements as long as the programs are open. Adware typically requires an active Internet connection to run.

QUESTION NO: 494

A program has been discovered that infects a critical Windows system executable and stays dormant in memory. When a Windows mobile phone is connected to the host, the program infects the phone's boot loader and continues to target additional Windows PCs or phones. Which of the following malware categories BEST describes this program?

- A. Zero-day
- B. Trojan
- C. Virus
- D. Rootkit

Answer: C

Explanation:

A computer virus is a program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man-made. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Some people distinguish between general viruses and worms. A worm is a special type of virus

that can replicate itself and use memory, but cannot attach itself to other programs.

QUESTION NO: 495

A user casually browsing the Internet is redirected to a warez site where a number of pop-ups appear. After clicking on a pop-up to complete a survey, a drive-by download occurs. Which of the following is MOST likely to be contained in the download?

- A. Backdoor
- B. Spyware
- C. Logic bomb
- D. DDoS
- E. Smurf

Answer: B

Explanation: Explanation

Spyware is software that is used to gather information about a person or organization without their knowledge and sends that information to another entity.

Whenever spyware is used for malicious purposes, its presence is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

QUESTION NO: 496

Which of the following malware types typically allows an attacker to monitor a user's computer, is characterized by a drive-by download, and requires no user interaction?

- A. Virus
- B. Logic bomb
- C. Spyware
- D. Adware

Answer: C

Explanation: Explanation

Spyware is software that is used to gather information about a person or organization without their knowledge and sends that information to another entity.

QUESTION NO: 497

Sara, a user, downloads a keygen to install pirated software. After running the keygen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following BEST describes this type of malware?

- A. Logic bomb
- B. Worm
- C. Trojan
- D. Adware

Answer: C

Explanation:

In computers, a Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan was a program that was supposed to find and destroy computer viruses. A Trojan horse may be widely redistributed as part of a computer virus.

QUESTION NO: 498

During a server audit, a security administrator does not notice abnormal activity. However, a network security analyst notices connections to unauthorized ports from outside the corporate network. Using specialized tools, the network security analyst also notices hidden processes running. Which of the following has MOST likely been installed on the server?

- A. SPIM
- B. Backdoor
- C. Logic bomb
- D. Rootkit

Answer: D

Explanation:

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer or computer network. Typically, a cracker installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password. Once the rootkit is installed, it allows the attacker to mask intrusion and gain root or privileged access to the computer and, possibly, other machines on the network.

A rootkit may consist of spyware and other programs that: monitor traffic and keystrokes; create a "backdoor" into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to escape detection.

The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun

and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

QUESTION NO: 499

A trojan was recently discovered on a server. There are now concerns that there has been a security breach that allows unauthorized people to access data. The administrator should be looking for the presence of a/an:

- A. Logic bomb.
- B. Backdoor.
- C. Adware application.
- D. Rootkit.

Answer: B

Explanation:

There has been a security breach on a computer system. The security administrator should now check for the existence of a backdoor.

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit.

A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.

Although the number of backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed.

Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission.

Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures—and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

QUESTION NO: 500

Two programmers write a new secure application for the human resources department to store

personal identifiable information. The programmers make the application available to themselves using an uncommon port along with an ID and password only they know. This is an example of which of the following?

- A. Root Kit
- B. Spyware
- C. Logic Bomb
- D. Backdoor

Answer: D

Explanation:

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit.

A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.

Although the number of backdoors in systems using proprietary software (software whose source code is not publicly available) is not widely credited, they are nevertheless frequently exposed.

Programmers have even succeeded in secretly installing large amounts of benign code as Easter eggs in programs, although such cases may involve official forbearance, if not actual permission.

Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such

backdoors appear to be installed so that spammers can send junk e-mail from the infected

machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs

through late 2005, are intended as DRM measures—and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

QUESTION NO: 501

The Chief Information Officer (CIO) receives an anonymous threatening message that says “beware of the 1st of the year”. The CIO suspects the message may be from a former disgruntled employee planning an attack.

Which of the following should the CIO be concerned with?

- A. Smurf Attack
- B. Trojan
- C. Logic bomb
- D. Virus

Answer: C

Explanation:

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs".

To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

QUESTION NO: 502

Ann, a software developer, has installed some code to reactivate her account one week after her account has been disabled. Which of the following is this an example of? (Select TWO).

- A. Rootkit
- B. Logic Bomb
- C. Botnet
- D. Backdoor
- E. Spyware

Answer: B,D

Explanation:

This is an example of both a logic bomb and a backdoor. The logic bomb is configured to 'go off' or activate one week after her account has been disabled. The reactivated account will provide a backdoor into the system.

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs".

To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set

time are not normally regarded as logic bombs.

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing unauthorized remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected. The backdoor may take the form of an installed program (e.g., Back Orifice) or may subvert the system through a rootkit.

A backdoor in a login system might take the form of a hard coded user and password combination which gives access to the system.

QUESTION NO: 503

Which of the following malware types is MOST likely to execute its payload after Jane, an employee, has left the company?

- A. Rootkit
- B. Logic bomb
- C. Worm
- D. Botnet

Answer: B

Explanation:

This is an example of a logic bomb. The logic bomb is configured to 'go off' or when Jane has left the company.

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files should they ever be terminated from the company.

Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Friday the 13th or April Fool's Day. Trojans that activate on certain dates are often called "time bombs".

To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software. As an example, trial programs with code that disables certain functionality after a set time are not normally regarded as logic bombs.

QUESTION NO: 504

Pete, a security analyst, has been tasked with explaining the different types of malware to his colleagues. The two malware types that the group seems to be most interested in are botnets and viruses. Which of the following explains the difference between these two types of malware?

- A. Viruses are a subset of botnets which are used as part of SYN attacks.
- B. Botnets are a subset of malware which are used as part of DDoS attacks.
- C. Viruses are a class of malware which create hidden openings within an OS.
- D. Botnets are used within DR to ensure network uptime and viruses are not.

Answer: B

Explanation:

A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks. The word botnet is a combination of the words robot and network. The term is usually used with a negative or malicious connotation.

Computers can be co-opted into a botnet when they execute malicious software. This can be accomplished by luring users into making a drive-by download, exploiting web browser vulnerabilities, or by tricking the user into running a Trojan horse program, which may come from an email attachment. This malware will typically install modules that allow the computer to be commanded and controlled by the botnet's operator. Many computer users are unaware that their computer is infected with bots. Depending on how it is written, a Trojan may then delete itself, or may remain present to update and maintain the modules.

QUESTION NO: 505

A user, Ann, is reporting to the company IT support group that her workstation screen is blank other than a window with a message requesting payment or else her hard drive will be formatted. Which of the following types of malware is on Ann's workstation?

- A. Trojan
- B. Spyware
- C. Adware
- D. Ransomware

Answer: D

Explanation:

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive), while some may simply lock the system and display messages intended to coax the user into paying.

Ransomware typically propagates as a trojan like a conventional computer worm, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program will then run a payload: such as one that will begin to encrypt personal files on the hard drive. More sophisticated ransomware may hybrid-encrypt the victim's plaintext with a random

symmetric key and a fixed public key. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to restrict interaction with the system, typically by setting the Windows Shell to itself, or even modifying the master boot record and/or partition table (which prevents the operating system from booting at all until it is repaired)

Ransomware payloads utilize elements of scareware to extort money from the system's user. The payload may, for example, display notices purportedly issued by companies or law enforcement agencies which falsely claim that the system had been used for illegal activities, or contains illegal content such as pornography and pirated software or media. Some ransomware payloads imitate Windows' product activation notices, falsely claiming that their computer's Windows installation is counterfeit or requires re-activation. These tactics coax the user into paying the malware's author to remove the ransomware, either by supplying a program which can decrypt the files, or by sending an unlock code that undoes the changes the payload has made.

QUESTION NO: 506

Which of the following describes a type of malware which is difficult to reverse engineer in a virtual lab?

- A.** Armored virus
- B.** Polymorphic malware
- C.** Logic bomb
- D.** Rootkit

Answer: A

Explanation:

An armored virus is a type of virus that has been designed to thwart attempts by analysts from examining its code by using various methods to make tracing, disassembling and reverse engineering more difficult. An Armored Virus may also protect itself from antivirus programs, making it more difficult to trace. To do this, the Armored Virus attempts to trick the antivirus program into believing its location is somewhere other than where it really is on the system.

QUESTION NO: 507 HOTSPOT

Select the appropriate attack from each drop down list to label the corresponding illustrated attack














Instructions: Attacks may only be used once, and will disappear from drop down list if selected.

When you have completed the simulation, please select the Done button to submit.

Question
Show

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.














Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	<input type="text"/>
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	<input type="text"/>
 Attacker collecting credit card details	 Phone-based victim	<input type="text"/>
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<input type="text"/>
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  Legitimate site </div> <div style="margin-right: 10px;">  Fraudulent site </div> </div>	<input type="text"/>

Reset All

Question
Show

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.














Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	<div style="border: 1px solid #ccc; padding: 2px;"> SPEAR PUSHING HOAX VISHING PHISHING PHARMING </div>
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	<div style="border: 1px solid #ccc; padding: 2px;"> SPEAR PUSHING HOAX VISHING PHISHING PHARMING </div>
 Attacker collecting credit card details	 Phone-based victim	<div style="border: 1px solid #ccc; padding: 2px;"> SPEAR PUSHING HOAX VISHING PHISHING PHARMING </div>
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	<div style="border: 1px solid #ccc; padding: 2px;"> SPEAR PUSHING HOAX VISHING PHISHING PHARMING </div>
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;">  Legitimate site </div> <div style="margin-right: 10px;">  Fraudulent site </div> </div>	<div style="border: 1px solid #ccc; padding: 2px;"> SPEAR PUSHING HOAX VISHING PHISHING PHARMING </div>

Reset All

Answer:

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.














Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker collecting credit card details	 Phone-based victim	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	SPEAR PUSHING HOAX VISHING PHISHING PHARMING
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims <div style="display: flex; align-items: center;">  Fraudulent site </div> <div style="display: flex; align-items: center;">  Legitimate site </div>	SPEAR PUSHING HOAX VISHING PHISHING PHARMING

Reset All

Explanation:

Attacks

Instructions: Attacks may only be used once, and will disappear from drop down list if selected.
When you have completed the simulation, please select the Done button to submit.

Attack Vector	Target	Identified Attack
 Attacker gains confidential company information	 Targeted CEO and board members	SPEAR PHISHING
 Attacker posts link to fake AV software	 Multiple social networks  Broad set of victims	HOAX
 Attacker collecting credit card details	 Phone-based victim	VISHING
 Attacker mass-mails product information to parties that have already opted out of receiving advertisements	 Broad set of recipients	PHISHING
 Attacker redirects name resolution entries from legitimate site to fraudulent site	 Victims <div style="display: flex; align-items: center;">  Fraudulent site </div> <div style="display: flex; align-items: center;">  Legitimate site </div>	PHARMING

Reset All

1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages

usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti-virus) software is genuine.

3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

References:

<http://searchsecurity.techtarget.com/definition/spear-phishing>

<http://www.webopedia.com/TERM/V/vishing.html>

<http://www.webopedia.com/TERM/P/phishing.html>

<http://www.webopedia.com/TERM/P/pharming.html>

QUESTION NO: 508 DRAG DROP

Determine the types of attacks below by selecting an option from the dropdown list.

Determine the types of Attacks from right to specific action.

Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.










	Email sent to multiple users to a link to verify username/password on external site		Choose Attack Type
	Phone calls made to CEO of organization asking for various financial data		Choose Attack Type
	Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone		Choose Attack Type
	You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet		Choose Attack Type
	A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.		Choose Attack Type

1. Phishing
2. Pharming
3. Vishing
4. Whaling
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
9. Spim
10. Social Engineering

Answer:

Types of attacks

Task: Determine the types of attacks below by selecting an option from the dropdown list.

	Email sent to multiple users to a link to verify username/password on external site		1. Phishing
	Phone calls made to CEO of organization asking for various financial data		4. Whaling
	Phone call is made to individual stating there was an IT issue, and asked for the user's password over the phone		3. Vishing
	You're on a social media site and an instant message pops up from a friend with a link to a new breakthrough diet		9. Spim
	A friend/colleague asks you questions of a personal nature, which could be considered typical password reset questions.		10. Social Engineering

1. Phishing
2. Pharming
3. Vishing
4. Whaling
5. X-Mas
6. Spoofing
7. Hoax
8. Spam
9. Spim
10. Social Engineering

Explanation:

- A. Phishing.
- B. Whaling.
- C. Vishing.
- D. Spim.
- E. Social engineering.

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS).

E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter.

A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

References:

<http://www.webopedia.com/TERM/P/phishing.html>

<http://www.techopedia.com/definition/28643/whaling>

<http://www.webopedia.com/TERM/V/vishing.html>

<http://searchsecurity.techtarget.com/definition/social-engineering>

QUESTION NO: 509

A server with the IP address of 10.10.2.4 has been having intermittent connection issues. The logs show repeated connection attempts from the following IPs:

10.10.3.16

10.10.3.23

212.178.24.26

217.24.94.83

These attempts are overloading the server to the point that it cannot respond to traffic. Which of the following attacks is occurring?

- A. XSS
- B. DDoS
- C. DoS
- D. Xmas

Answer: B

Explanation:

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be

accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

QUESTION NO: 510

A distributed denial of service attack can BEST be described as:

- A. Invalid characters being entered into a field in a database application.
- B. Users attempting to input random or invalid data into fields within a web browser application.
- C. Multiple computers attacking a single target in an organized attempt to deplete its resources.
- D. Multiple attackers attempting to gain elevated privileges on a target system.

Answer: C

Explanation:

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be

able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

QUESTION NO: 511

An administrator notices an unusual spike in network traffic from many sources. The administrator suspects that:

- A. it is being caused by the presence of a rogue access point.
- B. it is the beginning of a DDoS attack.
- C. the IDS has been compromised.
- D. the internal DNS tables have been poisoned.

Answer: B

Explanation:

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload.

A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further

interaction was necessary to launch the attack.

QUESTION NO: 512

A security technician at a small business is worried about the Layer 2 switches in the network suffering from a DoS style attack caused by staff incorrectly cabling network connections between switches.

Which of the following will BEST mitigate the risk if implemented on the switches?

- A. Spanning tree
- B. Flood guards
- C. Access control lists
- D. Syn flood

Answer: A

Explanation:

Spanning Tree is designed to eliminate network 'loops' from incorrect cabling between switches. Imagine two switches named switch 1 and switch 2 with two network cables connecting the switches. This would cause a network loop. A network loop between two switches can cause a 'broadcast storm' where a broadcast packet is sent out of all ports on switch 1 which includes two links to switch 2. The broadcast packet is then sent out of all ports on switch 2 which includes links back to switch 1. The broadcast packet will be sent out of all ports on switch 1 again which includes two links to switch 2 and so on thus flooding the network with broadcast traffic.

The Spanning-Tree Protocol (STP) was created to overcome the problems of transparent bridging in redundant networks. The purpose of STP is to avoid and eliminate loops in the network by negotiating a loop-free path through a root bridge. This is done by determining where there are loops in the network and blocking links that are redundant.

Spanning-Tree Protocol executes an algorithm called the Spanning-Tree Algorithm (STA). In order to find redundant links, STA will choose a reference point called a Root Bridge, and then determines all the available paths to that reference point. If it finds a redundant path, it chooses for the best path to forward and for all other redundant paths to block. This effectively severs the redundant links within the network.

All switches participating in STP gather information on other switches in the network through an exchange of data messages. These messages are referred to as Bridge Protocol Data Units (BPDUs). The exchange of BPDUs in a switched environment will result in the election of a root switch for the stable spanning-tree network topology, election of designated switch for every switched segment, and the removal of loops in the switched network by placing redundant switch ports in a backup state.

QUESTION NO: 513

An administrator is assigned to monitor servers in a data center. A web server connected to the Internet suddenly experiences a large spike in CPU activity. Which of the following is the MOST likely cause?

- A. Spyware
- B. Trojan
- C. Privilege escalation
- D. DoS

Answer: D

Explanation:

A Distributed Denial of Service (DDoS) attack is a DoS attack from multiple computers whereas a DoS attack is from a single computer. In terms of the actual method of attack, DDoS and DoS attacks are the same.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

Malware can carry DDoS attack mechanisms; one of the better-known examples of this was MyDoom. Its DoS mechanism was triggered on a specific date and time. This type of DDoS involved hardcoding the target IP address prior to release of the malware and no further interaction was necessary to launch the attack.

QUESTION NO: 514

Which of the following attacks could be used to initiate a subsequent man-in-the-middle attack?

- A. ARP poisoning
- B. DoS
- C. Replay
- D. Brute force

Answer: C

Explanation:

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation.

Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication.

One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems.

Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check.

Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if

they are performed quickly enough i.e. within that 'reasonable' limit, could succeed.

QUESTION NO: 515

A network analyst received a number of reports that impersonation was taking place on the network. Session tokens were deployed to mitigate this issue and defend against which of the following attacks?

- A. Replay
- B. DDoS
- C. Smurf
- D. Ping of Death

Answer: A

Explanation:

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation.

Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication.

One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions

in addition to sessions. The technique has been widely implemented in personal online banking systems.

Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check.

Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed.

QUESTION NO: 516

Timestamps and sequence numbers act as countermeasures against which of the following types of attacks?

- A. Smurf
- B. DoS
- C. Vishing
- D. Replay

Answer: D

Explanation:

A replay attack (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack by IP packet substitution (such as stream cipher attack).

For example: Suppose Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping on the conversation and keeps the password (or the hash). After the interchange is over, Eve (posing as Alice) connects to Bob; when asked for a proof of identity, Eve sends Alice's password (or hash) read from the last session, which Bob accepts thus granting access to Eve.

Countermeasures: A way to avoid replay attacks is by using session tokens: Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob

performs the same computation; if and only if both values match, the login is successful. Now suppose Eve has captured this value and tries to use it on another session; Bob sends a different session token, and when Eve replies with the captured value it will be different from Bob's computation.

Session tokens should be chosen by a (pseudo-) random process. Otherwise Eve may be able to pose as Bob, presenting some predicted future token, and convince Alice to use that token in her transformation. Eve can then replay her reply at a later time (when the previously predicted token is actually presented by Bob), and Bob will accept the authentication.

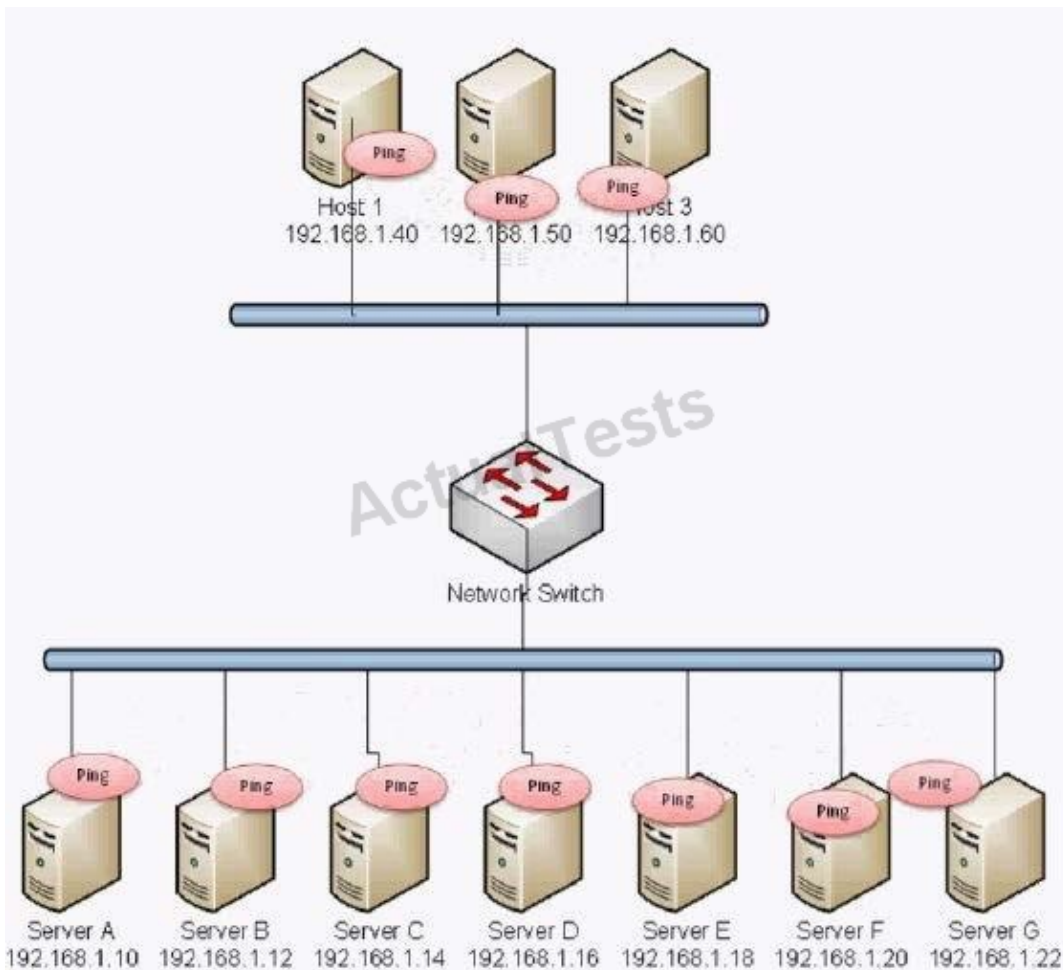
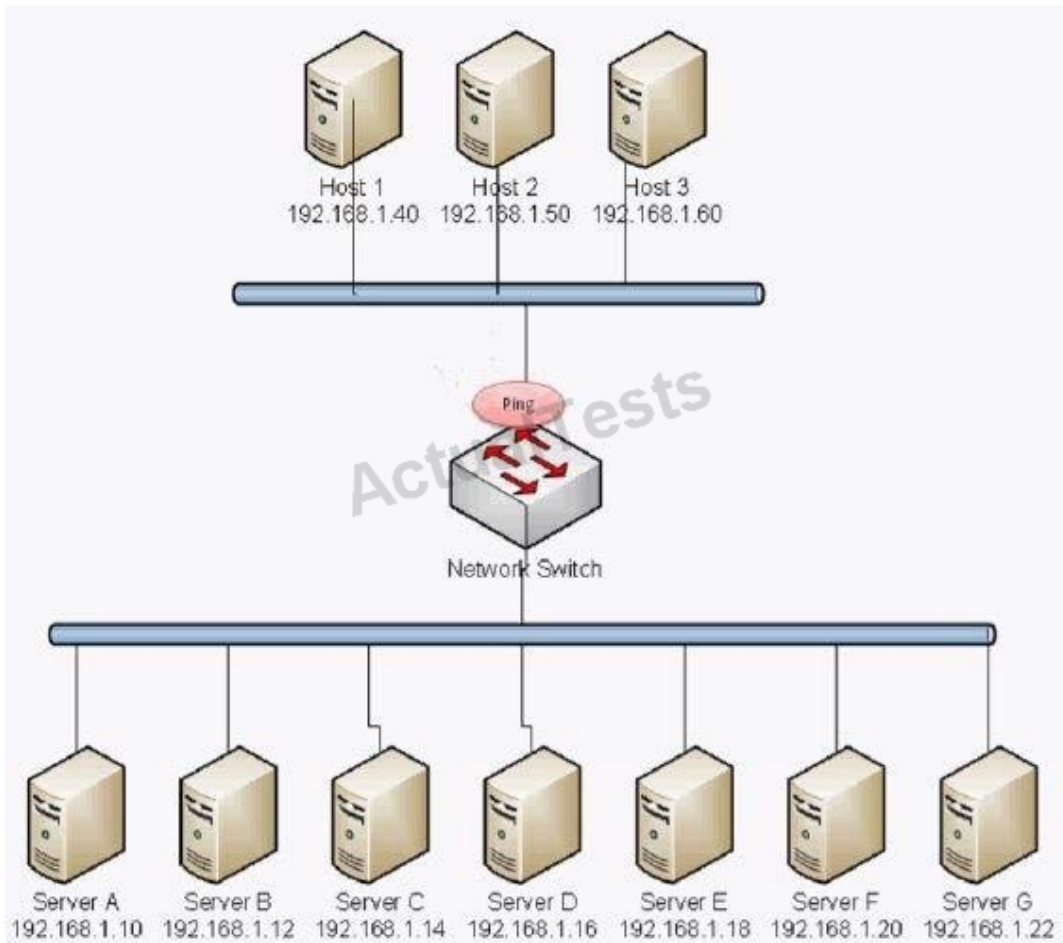
One-time passwords are similar to session tokens in that the password expires after it has been used or after a very short amount of time. They can be used to authenticate individual transactions in addition to sessions. The technique has been widely implemented in personal online banking systems.

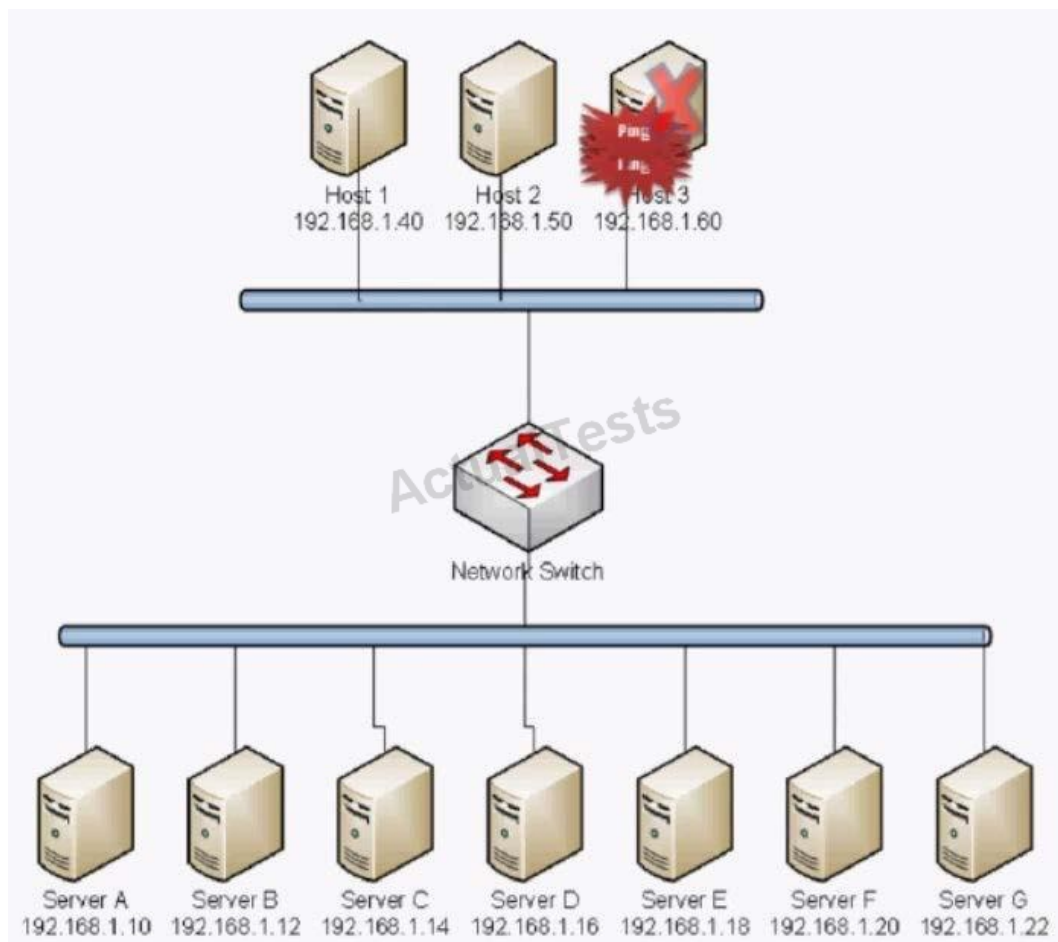
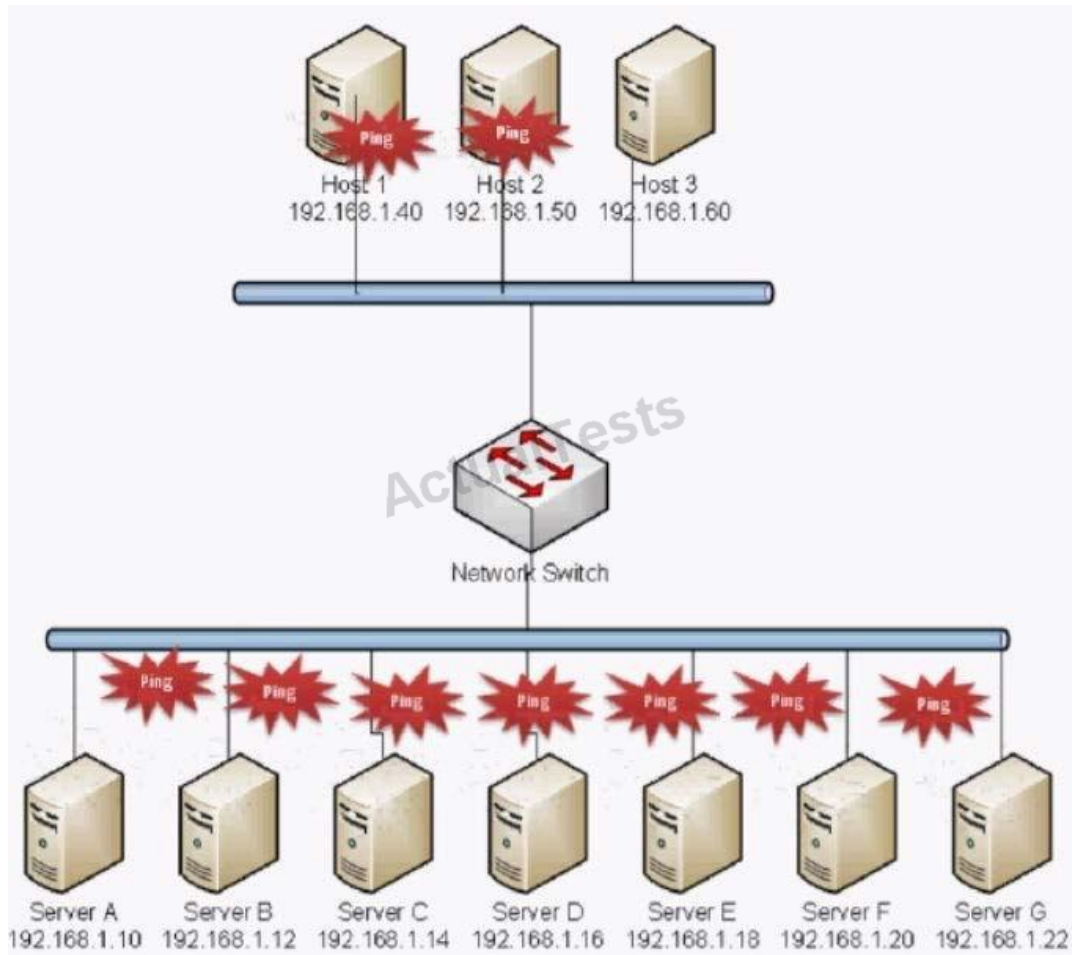
Bob can also send nonces but should then include a message authentication code (MAC), which Alice should check.

Timestamping is another way of preventing a replay attack. Synchronization should be achieved using a secure protocol. For example Bob periodically broadcasts the time on his clock together with a MAC. When Alice wants to send Bob a message, she includes her best estimate of the time on his clock in her message, which is also authenticated. Bob only accepts messages for which the timestamp is within a reasonable tolerance. The advantage of this scheme is that Bob does not need to generate (pseudo-) random numbers, with the trade-off being that replay attacks, if they are performed quickly enough i.e. within that 'reasonable' limit, could succeed.

QUESTION NO: 517

Which of the following BEST describes the type of attack that is occurring?





- A. Smurf Attack
- B. Man in the middle
- C. Backdoor
- D. Replay
- E. Spear Phishing
- F. Xmas Attack
- G. Blue Jacking
- H. Ping of Death

Answer: A

Explanation:

The exhibit shows that all the computers on the network are being 'pinged'. This indicates that the ping request was sent to the network broadcast address. We can also see that all the replies were received by one (probably with a spoofed address) host on the network. This is typical of a smurf attack.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

QUESTION NO: 518

Which of the following will help prevent smurf attacks?

- A. Allowing necessary UDP packets in and out of the network
- B. Disabling directed broadcast on border routers
- C. Disabling unused services on the gateway firewall
- D. Flash the BIOS with the latest firmware

Answer: B

Explanation:

A smurf attack involves sending PING requests to a broadcast address. Therefore, we can prevent

smurf attacks by blocking broadcast packets on our external routers.

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

QUESTION NO: 519

Which of the following wireless security measures can an attacker defeat by spoofing certain properties of their network interface card?

- A. WEP
- B. MAC filtering
- C. Disabled SSID broadcast
- D. TKIP

Answer: B

Explanation:

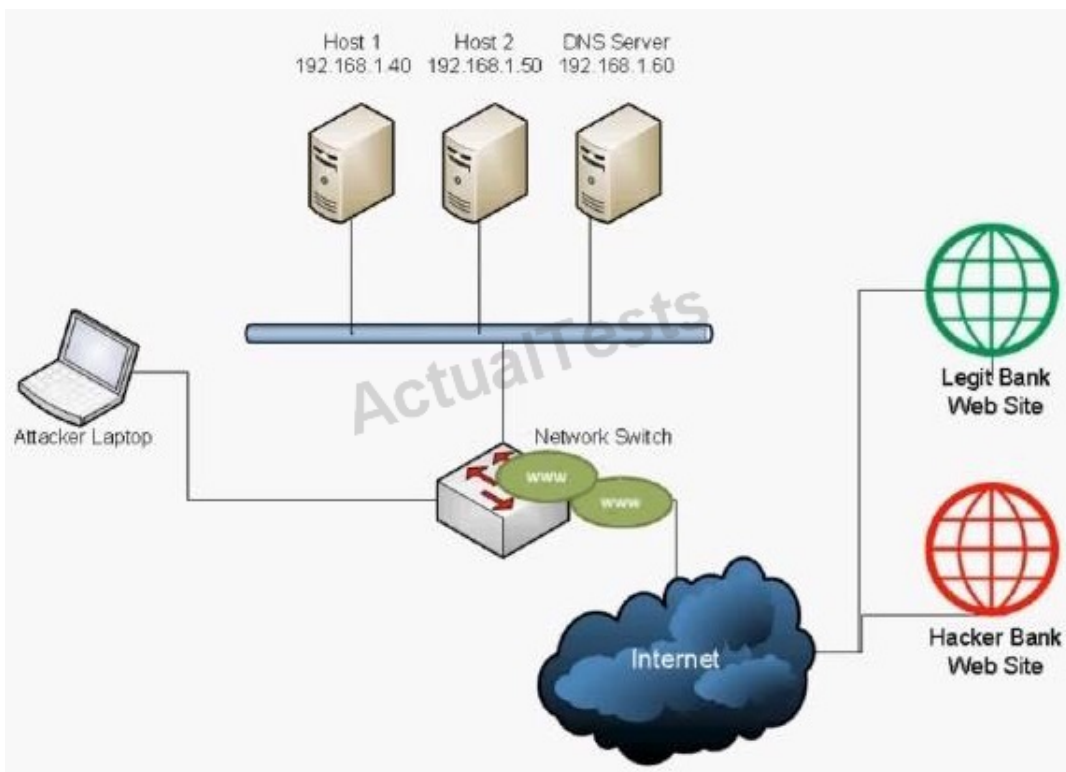
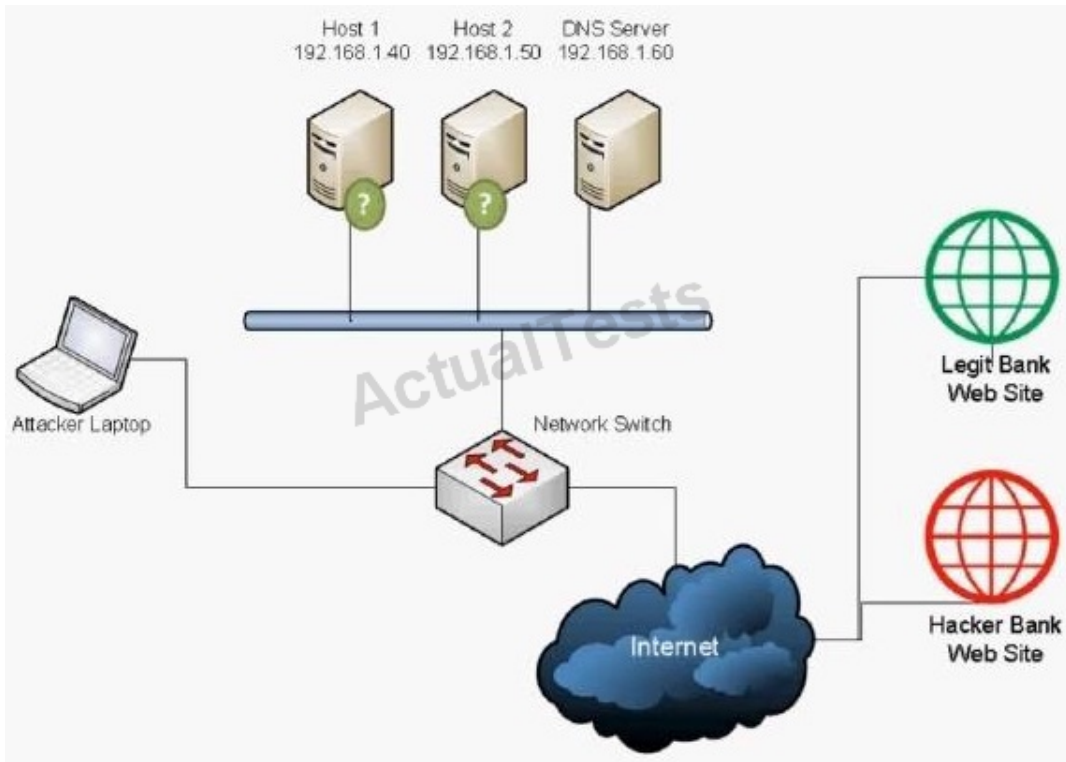
MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

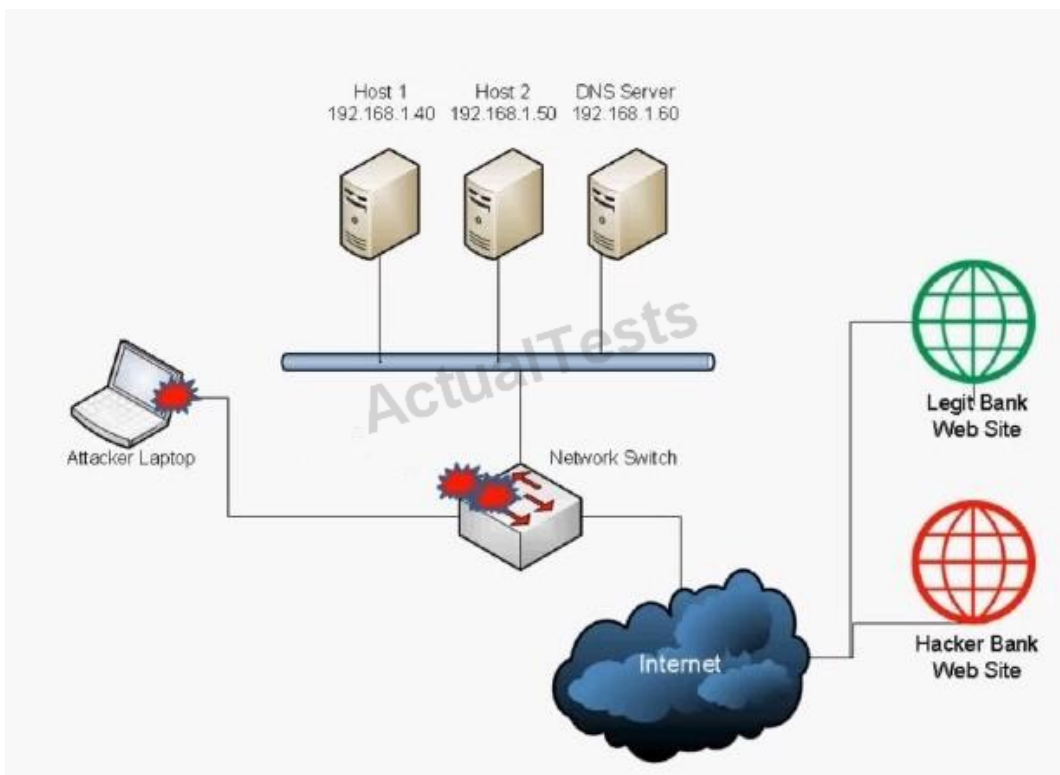
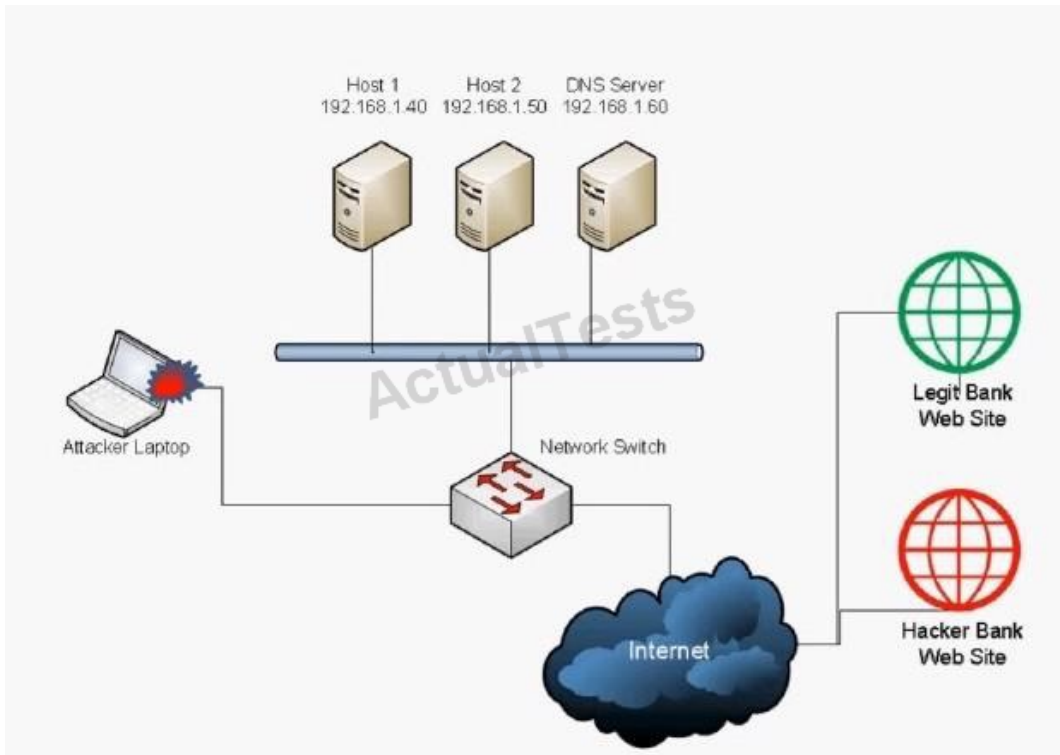
MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

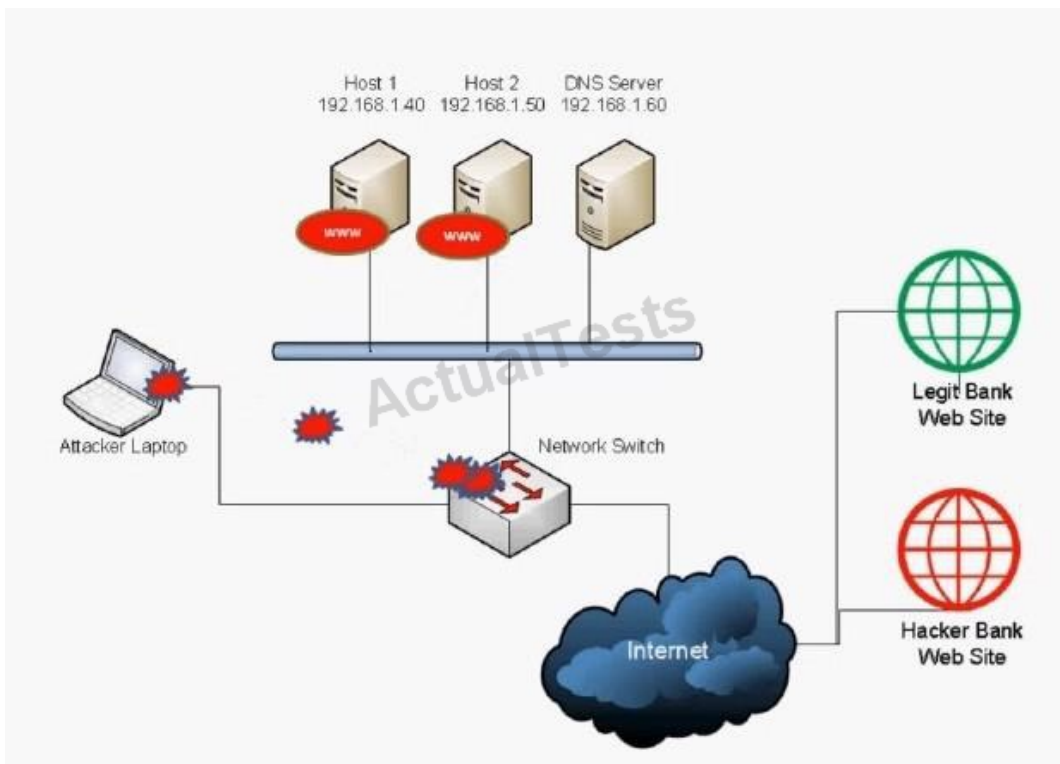
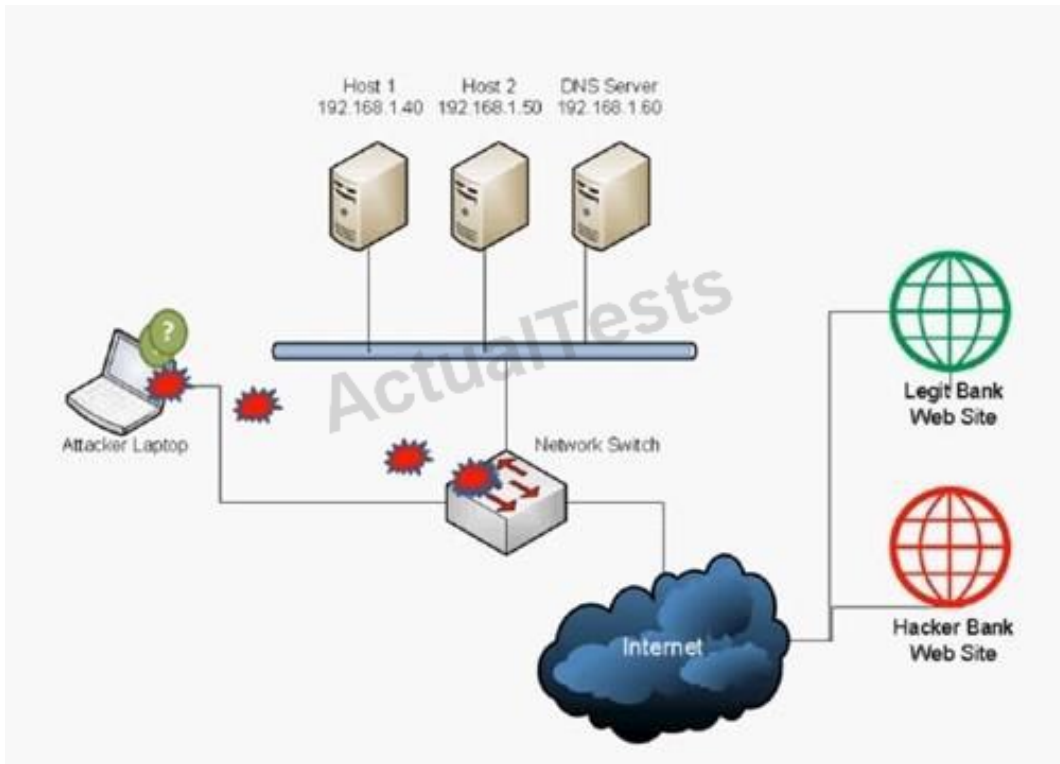
While giving a wireless network some additional protection, MAC filtering can be circumvented by scanning a valid MAC (via airodumping) and then spoofing one's own MAC into a validated one.

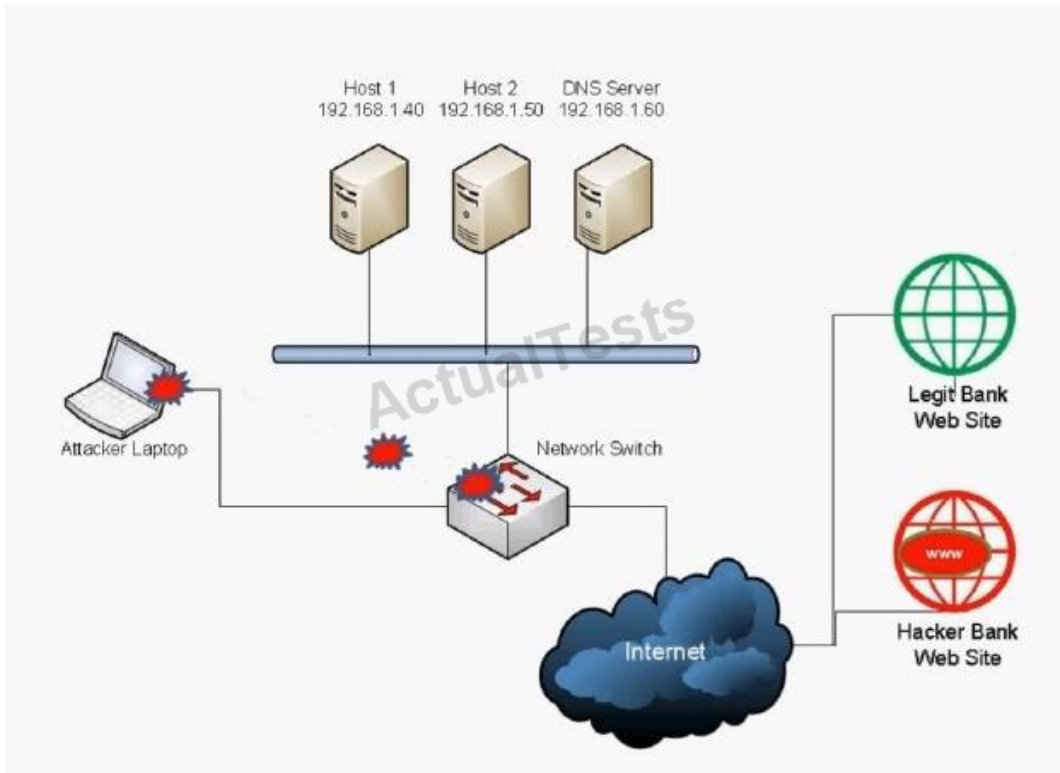
QUESTION NO: 520

Which of the following BEST describes the type of attack that is occurring? (Select TWO).









- A. DNS spoofing
- B. Man-in-the-middle
- C. Backdoor
- D. Replay
- E. ARP attack
- F. Spear phishing
- G. Xmas attack

Answer: A,E

Explanation:

We have a legit bank web site and a hacker bank web site. The hacker has a laptop connected to the network. The hacker is redirecting bank web site users to the hacker bank web site instead of the legit bank web site. This can be done using two methods: DNS Spoofing and ARP Attack (ARP Poisoning).

A: DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer). A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other server again.

When a DNS server has received a false translation and caches it for performance optimization, it

is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the hacker bank web site server).

E: Address Resolution Protocol poisoning (ARP poisoning) is a form of attack in which an attacker changes the Media Access Control (MAC) address and attacks an Ethernet LAN by changing the target computer's ARP cache with a forged ARP request and reply packets. This modifies the layer -Ethernet MAC address into the hacker's known MAC address to monitor it. Because the ARP replies are forged, the target computer unintentionally sends the frames to the hacker's computer first instead of sending it to the original destination. As a result, both the user's data and privacy are compromised. An effective ARP poisoning attempt is undetectable to the user. ARP poisoning is also known as ARP cache poisoning or ARP poison routing (APR).

QUESTION NO: 521

Mike, a user, states that he is receiving several unwanted emails about home loans. Which of the following is this an example of?

- A. Spear phishing
- B. Hoaxes
- C. Spoofing
- D. Spam

Answer: D

Explanation:

Spam is most often considered to be electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited email. However, if a long-lost brother finds your email address and sends you a message, this could hardly be called spam, even though it is unsolicited. Real spam is generally email advertising for some product sent to a mailing list or newsgroup.

In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth. Consequently, there are many organizations, as well as individuals, who have taken it upon themselves to fight spam with a variety of techniques. But because the Internet is public, there is really little that can be done to prevent spam, just as it is impossible to prevent junk mail. However, some online services have instituted policies to prevent spammers from spamming their subscribers.

There is some debate about why it is called spam, but the generally accepted version is that it comes from the Monty Python song, "Spam spam spam spam, spam spam spam spam, lovely spam, wonderful spam". Like the song, spam is an endless repetition of worthless text. Another school of thought maintains that it comes from the computer group lab at the University of

Southern California who gave it the name because it has many of the same characteristics as the lunch meat Spam:

Nobody wants it or ever asks for it.

No one ever eats it; it is the first item to be pushed to the side when eating the entree.

Sometimes it is actually tasty, like 1% of junk mail that is really useful to some people.

The term spam can also be used to describe any "unwanted" email from a company or website -- typically at some point a user would have agreed to receive the email via subscription list opt-in -- a newer term called graymail is used to describe this particular type of spam.

QUESTION NO: 522

Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?

- A.** Trojan virus
- B.** Botnet
- C.** Worm outbreak
- D.** Logic bomb

Answer: C

Explanation:

A worm is similar to a virus but is typically less malicious. A virus will usually cause damage to the system or files whereas a worm will usually just spread itself either using the network or by sending emails.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

QUESTION NO: 523

A security administrator notices large amounts of traffic within the network heading out to an external website. The website seems to be a fake bank site with a phone number that when called, asks for sensitive information. After further investigation, the security administrator notices that a fake link was sent to several users. This is an example of which of the following attacks?

- A.** Vishing

- B. Phishing
- C. Whaling
- D. SPAM
- E. SPIM

Answer: B

Explanation:

Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

Phishing emails are blindly sent to thousands, if not millions of recipients. By spamming large groups of people, the "phisher" counts on the email being read by a percentage of people who actually have an account with the legitimate company being spoofed in the email and corresponding webpage.

Phishing, also referred to as brand spoofing or carding, is a variation on "fishing," the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.

QUESTION NO: 524

Jane, an individual, has recently been calling various financial offices pretending to be another person to gain financial information. Which of the following attacks is being described?

- A. Phishing
- B. Tailgating
- C. Pharming
- D. Vishing

Answer: D

Explanation:

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or

other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless.

Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

QUESTION NO: 525

Purchasing receives an automated phone call from a bank asking to input and verify credit card information. The phone number displayed on the caller ID matches the bank. Which of the following attack types is this?

- A. Hoax
- B. Phishing
- C. Vishing
- D. Whaling

Answer: C

Explanation:

Vishing (voice or VoIP phishing) is an electronic fraud tactic in which individuals are tricked into revealing critical financial or personal information to unauthorized entities. Vishing works like phishing but does not always occur over the Internet and is carried out using voice technology. A vishing attack can be conducted by voice email, VoIP (voice over IP), or landline or cellular telephone.

The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless.

Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

QUESTION NO: 526

A company's employees were victims of a spear phishing campaign impersonating the CEO. The company would now like to implement a solution to improve the overall security posture by assuring their employees that email originated from the CEO. Which of the following controls could they implement to BEST meet this goal?

- A. Spam filter
- B. Digital signatures
- C. Antivirus software
- D. Digital certificates

Answer: B

Explanation:

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document.

The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one-way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm -- is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

QUESTION NO: 527

A user has unknowingly gone to a fraudulent site. The security analyst notices the following system change on the user's host:

Old `hosts' file:

127.0.0.1 localhost

New `hosts' file:

127.0.0.1 localhost

5.5.5.5 www.comptia.com

Which of the following attacks has taken place?

- A. Spear phishing
- B. Pharming
- C. Phishing
- D. Vishing

Answer: B

Explanation:

We can see in this question that a fraudulent entry has been added to the user's hosts file. This will point the URL: www.comptia.com to 5.5.5.5 instead of the correct IP address.

Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server (or hosts file) by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.

QUESTION NO: 528

Users at a company report that a popular news website keeps taking them to a web page with

derogatory content. This is an example of which of the following?

- A. Evil twin
- B. DNS poisoning
- C. Vishing
- D. Session hijacking

Answer: B

Explanation:

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other server again.

When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the server hosting the web page with derogatory content).

QUESTION NO: 529

Which of the following is described as an attack against an application using a malicious file?

- A. Client side attack
- B. Spam
- C. Impersonation attack
- D. Phishing attack

Answer: A

Explanation:

In this question, a malicious file is used to attack an application. If the application is running on a client computer, this would be a client side attack. Attacking a service or application on a server would be a server side attack.

Client-side attacks target vulnerabilities in client applications interacting with a malicious data. The difference is the client is the one initiating the bad connection.

Client-side attacks are becoming more popular. This is because server side attacks are not as

easy as they once were according to apache.org.

Attackers are finding success going after weaknesses in desktop applications such as browsers, media players, common office applications and e-mail clients.

To defend against client-side attacks keep-up the most current application patch levels, keep antivirus software updated and keep authorized software to a minimum.

QUESTION NO: 530

Which of the following would BEST deter an attacker trying to brute force 4-digit PIN numbers to access an account at a bank teller machine?

- A.** Account expiration settings
- B.** Complexity of PIN
- C.** Account lockout settings
- D.** PIN history requirements

Answer: C

Explanation:

Account lockout settings determine the number of failed login attempts before the account gets locked and how long the account will be locked out for. For example, an account can be configured to lock if three incorrect passwords (or in this case PIN's) are entered. The account can then be configured to automatically unlock after a period of time or stay locked until someone manually unlocks it.

QUESTION NO: 531

Which of the following can be used by a security administrator to successfully recover a user's forgotten password on a password protected file?

- A.** Cognitive password
- B.** Password sniffing
- C.** Brute force
- D.** Social engineering

Answer: C

Explanation:

One way to recover a user's forgotten password on a password protected file is to guess it. A brute force attack is an automated attempt to open the file by using many different passwords.

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack may also be referred to as brute force cracking.

For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.

An attack of this nature can be time- and resource-consuming. Hence the name "brute force attack;" success is usually based on computing power and the number of combinations tried rather than an ingenious algorithm.

QUESTION NO: 532

A security administrator must implement all requirements in the following corporate policy: Passwords shall be protected against offline password brute force attacks. Passwords shall be protected against online password brute force attacks. Which of the following technical controls must be implemented to enforce the corporate policy? (Select THREE).

- A. Account lockout
- B. Account expiration
- C. Screen locks
- D. Password complexity
- E. Minimum password lifetime
- F. Minimum password length

Answer: A,D,F

Explanation:

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.

A brute force attack may also be referred to as brute force cracking.

For example, a form of brute force attack known as a dictionary attack might try all the words in a dictionary. Other forms of brute force attack might try commonly-used passwords or combinations of letters and numbers.

The best defense against brute force attacks strong passwords. The following password policies will ensure that users have strong (difficult to guess) passwords:

F: Minimum password length. This policy specifies the minimum number of characters a password should have. For example: a minimum password length of 8 characters is regarded as good security practice.

D: Password complexity determines what characters a password should include. For example, you could require a password to contain uppercase and lowercase letters and numbers. This will ensure that passwords don't consist of dictionary words which are easy to crack using brute force techniques.

A: Account lockout policy: This policy ensures that a user account is locked after a number of incorrect password entries. For example, you could specify that if a wrong password is entered three times, the account will be locked for a period of time or indefinitely until the account is unlocked by an administrator.

QUESTION NO: 533

A recent spike in virus detections has been attributed to end-users visiting www.compnay.com. The business has an established relationship with an organization using the URL of www.company.com but not with the site that has been causing the infections. Which of the following would BEST describe this type of attack?

- A. Typo squatting
- B. Session hijacking
- C. Cross-site scripting
- D. Spear phishing

Answer: A

Explanation:

Typosquatting, also called URL hijacking or fake url, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL (including an alternative website owned by a cybersquatter).

The typosquatter's URL will usually be one of four kinds, all similar to the victim site address: (In the following, the intended website is "example.com")

A common misspelling, or foreign language spelling, of the intended site: exemple.com

A misspelling based on typing errors: xample.com or examlpe.com

A differently phrased domain name: examples.com

A different top-level domain: example.org

Once in the typosquatter's site, the user may also be tricked into thinking that they are in fact in the real site; through the use of copied or similar logos, website layouts or content.

QUESTION NO: 534

Using proximity card readers instead of the traditional key punch doors would help to mitigate:

- A. Impersonation
- B. Tailgating
- C. Dumpster diving
- D. Shoulder surfing

Answer: D

Explanation:

Using a traditional key punch door, a person enters a code into a keypad to unlock the door. Someone could be watching the code being entered. They would then be able to open the door by entering the code. The process of watching the key code being entered is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

QUESTION NO: 535

Ann an employee is visiting Joe, an employee in the Human Resources Department. While talking to Joe, Ann notices a spreadsheet open on Joe's computer that lists the salaries of all employees in her department. Which of the following forms of social engineering would BEST describe this situation?

- A. Impersonation
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

Answer: D

Explanation:

Ann was able to see the Spreadsheet on Joe's computer. This direct observation is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

QUESTION NO: 536

An investigator recently discovered that an attacker placed a remotely accessible CCTV camera in a public area overlooking several Automatic Teller Machines (ATMs). It is also believed that user accounts belonging to ATM operators may have been compromised. Which of the following attacks has MOST likely taken place?

- A. Shoulder surfing
- B. Dumpster diving
- C. Whaling attack
- D. Vishing attack

Answer: A

Explanation:

The CCTV camera has recorded people entering their PINs in the ATMs. This is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

QUESTION NO: 537

All executive officers have changed their monitor location so it cannot be easily viewed when passing by their offices. Which of the following attacks does this action remediate?

- A. Dumpster Diving
- B. Impersonation
- C. Shoulder Surfing
- D. Whaling

Answer: C

Explanation:

Viewing confidential information on someone's monitor is known as shoulder surfing. By moving their monitors so they cannot be seen, the executives are preventing users passing by 'shoulder surfing'.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

QUESTION NO: 538

Ann, an employee, is cleaning out her desk and disposes of paperwork containing confidential customer information in a recycle bin without shredding it first. This is MOST likely to increase the risk of loss from which of the following attacks?

- A. Shoulder surfing
- B. Dumpster diving
- C. Tailgating
- D. Spoofing

Answer: B

Explanation:

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords

written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

QUESTION NO: 539

Several bins are located throughout a building for secure disposal of sensitive information.

Which of the following does this prevent?

- A. Dumpster diving
- B. War driving
- C. Tailgating
- D. War chalking

Answer: A

Explanation:

The bins in this question will be secure bins designed to prevent someone accessing the 'rubbish' to learn sensitive information.

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

QUESTION NO: 540

Physical documents must be incinerated after a set retention period is reached. Which of the following attacks does this action remediate?

- A. Shoulder Surfing

- B. Dumpster Diving
- C. Phishing
- D. Impersonation

Answer: B

Explanation:

Incinerating documents (or shredding documents) instead of throwing them into a bin will prevent people being able to read the documents to view sensitive information.

Dumpster diving is looking for treasure in someone else's trash. (A dumpster is a large trash container.) In the world of information technology, dumpster diving is a technique used to retrieve information that could be used to carry out an attack on a computer network. Dumpster diving isn't limited to searching through the trash for obvious treasures like access codes or passwords written down on sticky notes. Seemingly innocent information like a phone list, calendar, or organizational chart can be used to assist an attacker using social engineering techniques to gain access to the network. To prevent dumpster divers from learning anything valuable from your trash, experts recommend that your company establish a disposal policy where all paper, including print-outs, is shredded in a cross-cut shredder before being recycled, all storage media is erased, and all staff is educated about the danger of untracked trash.

QUESTION NO: 541

At the outside break area, an employee, Ann, asked another employee to let her into the building because her badge is missing. Which of the following does this describe?

- A. Shoulder surfing
- B. Tailgating
- C. Whaling
- D. Impersonation

Answer: B

Explanation:

Although Ann is an employee and therefore authorized to enter the building, she does not have her badge and therefore strictly she should not be allowed to enter the building.

Just as a driver can tailgate another driver's car by following too closely, in the security sense, tailgating means to compromise physical security by following somebody through a door meant to keep out intruders. Tailgating is actually a form of social engineering, whereby someone who is not authorized to enter a particular area does so by following closely behind someone who is authorized.

QUESTION NO: 542

Pete's corporation has outsourced help desk services to a large provider. Management has published a procedure that requires all users, when receiving support, to call a special number.

Users then need to enter the code provided to them by the help desk technician prior to allowing the technician to work on their PC. Which of the following does this procedure prevent?

- A. Collusion
- B. Impersonation
- C. Pharming
- D. Transitive Access

Answer: B

Explanation:

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

The procedure the users have to go through is to ensure that the technician who will have access to the computer is a genuine technician and not someone impersonating a technician.

QUESTION NO: 543

Purchasing receives a phone call from a vendor asking for a payment over the phone. The phone number displayed on the caller ID matches the vendor's number. When the purchasing agent asks to call the vendor back, they are given a different phone number with a different area code.

Which of the following attack types is this?

- A. Hoax
- B. Impersonation
- C. Spear phishing
- D. Whaling

Answer: B

Explanation:

In this question, the impersonator is impersonating a vendor and asking for payment. They have managed to 'spoof' their calling number so that their caller ID matches the vendor's number.

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server

applications. However, it can also be used as a security threat.

QUESTION NO: 544

A database administrator receives a call on an outside telephone line from a person who states that they work for a well-known database vendor. The caller states there have been problems applying the newly released vulnerability patch for their database system, and asks what version is being used so that they can assist. Which of the following is the BEST action for the administrator to take?

- A.** Thank the caller, report the contact to the manager, and contact the vendor support line to verify any reported patch issues.
- B.** Obtain the vendor's email and phone number and call them back after identifying the number of systems affected by the patch.
- C.** Give the caller the database version and patch level so that they can receive help applying the patch.
- D.** Call the police to report the contact about the database systems, and then check system logs for attack attempts.

Answer: A

Explanation:

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

In this question, the person making the call may be impersonating someone who works for a well-known database vendor. The actions described in this answer would mitigate the risk. By not divulging information about your database system and contacting the vendor directly, you can be sure that you are talking to the right people.

QUESTION NO: 545

A security administrator forgets their card to access the server room. The administrator asks a coworker if they could use their card for the day. Which of the following is the administrator using to gain access to the server room?

- A.** Man-in-the-middle
- B.** Tailgating
- C.** Impersonation
- D.** Spoofing

Answer: C

Explanation:

Impersonation is where a person, computer, software application or service pretends to be someone or something it's not. Impersonation is commonly non-maliciously used in client/server applications. However, it can also be used as a security threat.

In this question, by using the coworker's card, the security administrator is 'impersonating' the coworker. The server room locking system and any logging systems will 'think' that the coworker has entered the server room.

QUESTION NO: 546

Sara, an attacker, is recording a person typing in their ID number into a keypad to gain access to the building. Sara then calls the helpdesk and informs them that their PIN no longer works and would like to change it. Which of the following attacks occurred LAST?

- A. Phishing
- B. Shoulder surfing
- C. Impersonation
- D. Tailgating

Answer: C

Explanation:

Two attacks took place in this question. The first attack was shoulder surfing. This was the act of Sara recording a person typing in their ID number into a keypad to gain access to the building. The second attack was impersonation. Sara called the helpdesk and used the PIN to impersonate the person she recorded.

QUESTION NO: 547

Which of the following is characterized by an attacker attempting to map out an organization's staff hierarchy in order to send targeted emails?

- A. Whaling
- B. Impersonation
- C. Privilege escalation
- D. Spear phishing

Answer: A

Explanation:

A whaling attack is targeted at company executives. Mapping out an organization's staff hierarchy to determine who the people at the top are is also part of a whaling attack.

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

QUESTION NO: 548

Which of the following attacks targets high level executives to gain company information?

- A. Phishing
- B. Whaling
- C. Vishing
- D. Spoofing

Answer: B**Explanation:**

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

QUESTION NO: 549

Users are encouraged to click on a link in an email to obtain exclusive access to the newest version of a popular Smartphone. This is an example of.

- A. Scarcity
- B. Familiarity
- C. Intimidation
- D. Trust

Answer: A

Explanation:

Scarcity, in the area of social psychology, works much like scarcity in the area of economics. Simply put, humans place a higher value on an object that is scarce, and a lower value on those that are abundant. The thought that we, as humans, want something we cannot have drives us to desire the object even more. This idea is deeply embedded in the intensely popular, "Black Friday" shopping extravaganza that U.S. consumers participate in every year on the day after Thanksgiving. More than getting a bargain on a hot gift idea, shoppers thrive on the competition itself, in obtaining the scarce product.

In this question, people want the brand new latest version of a smartphone. The temptation of being one of the first to get the new phone will tempt people into clicking the link in the email.

QUESTION NO: 550

A computer supply company is located in a building with three wireless networks. The system security team implemented a quarterly security scan and saw the following.

SSIDStateChannelLevel

Computer AreUs1connected170dbm

Computer AreUs2connected580dbm

Computer AreUs3connected375dbm

Computer AreUs4connected695dbm

Which of the following is this an example of?

- A. Rogue access point
- B. Near field communication

- C. Jamming
- D. Packet sniffing

Answer: A

Explanation:

The question states that the building has three wireless networks. However, the scan is showing four wireless networks with the SSIDs: Computer AreUs1 , Computer AreUs2 , Computer AreUs3 and Computer AreUs4. Therefore, one of these wireless networks probably shouldn't be there.

This is an example of a rogue access point.

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

QUESTION NO: 551

Pete, the security engineer, would like to prevent wireless attacks on his network. Pete has implemented a security control to limit the connecting MAC addresses to a single port. Which of the following wireless attacks would this address?

- A. Interference
- B. Man-in-the-middle
- C. ARP poisoning
- D. Rogue access point

Answer: D

Explanation:

MAC filtering is typically used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists.

In this question, a rogue access point would need to be able to connect to the network to provide

access to network resources. If the MAC address of the rogue access point isn't allowed to connect to the network port, then the rogue access point will not be able to connect to the network.

QUESTION NO: 552

Users have been reporting that their wireless access point is not functioning. They state that it allows slow connections to the internet, but does not provide access to the internal network. The user provides the SSID and the technician logs into the company's access point and finds no issues. Which of the following should the technician do?

- A. Change the access point from WPA2 to WEP to determine if the encryption is too strong
- B. Clear all access logs from the AP to provide an up-to-date access list of connected users
- C. Check the MAC address of the AP to which the users are connecting to determine if it is an imposter
- D. Reconfigure the access point so that it is blocking all inbound and outbound traffic as a troubleshooting gap

Answer: C

Explanation:

The users may be connecting to a rogue access point. The rogue access point could be hosting a wireless network that has the same SSID as the corporate wireless network. The only way to tell for sure if the access point the users are connecting to is the correct one is to check the MAC address. Every network card has a unique 48-bit address assigned.

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and WiFi. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A network node may have multiple NICs and each NIC must have a unique MAC address. MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64.

QUESTION NO: 553

Ann, the network administrator, has learned from the helpdesk that employees are accessing the wireless network without entering their domain credentials upon connection. Once the connection is made, they cannot reach any internal resources, while wired network connections operate smoothly. Which of the following is MOST likely occurring?

- A. A user has plugged in a personal access point at their desk to connect to the network wirelessly.
- B. The company is currently experiencing an attack on their internal DNS servers.
- C. The company's WEP encryption has been compromised and WPA2 needs to be implemented instead.
- D. An attacker has installed an access point nearby in an attempt to capture company information.

Answer: D

Explanation:

The question implies that users should be required to enter their domain credentials upon connection to the wireless network. The fact that they are connecting to a wireless network without being prompted for their domain credentials and they are unable to access network resources suggests they are connecting to a rogue wireless network.

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

QUESTION NO: 554

Which of the following is where an unauthorized device is found allowing access to a network?

- A. Bluesnarfing
- B. Rogue access point
- C. Honeypot
- D. IV attack

Answer: B

Explanation:

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

QUESTION NO: 555

Which of the following attacks would cause all mobile devices to lose their association with corporate access points while the attack is underway?

- A. Wireless jamming
- B. Evil twin
- C. Rogue AP
- D. Packet sniffing

Answer: A

Explanation:

When most people think of frequency jamming, what comes to mind are radio, radar and cell phone jamming. However, any communication that uses radio frequencies can be jammed by a strong radio signal in the same frequency. In this manner, Wi-Fi may be attacked with a network jamming attack, reducing signal quality until it becomes unusable or disconnects occur. With very similar methods, a focused and aimed signal can actually break access point hardware, as with equipment destruction attacks.

QUESTION NO: 556

The system administrator has been notified that many users are having difficulty connecting to the company's wireless network. They take a new laptop and physically go to the access point and connect with no problems. Which of the following would be the MOST likely cause?

- A. The certificate used to authenticate users has been compromised and revoked.
- B. Multiple war drivers in the parking lot have exhausted all available IPs from the pool to deny access.
- C. An attacker has gained access to the access point and has changed the encryption keys.
- D. An unauthorized access point has been configured to operate on the same channel.

Answer: D

Explanation:

Wireless Access Points can be configured to use a channel. If you have multiple access points within range of each other, you should configure the access points to use different channels. Different channels use different frequencies. If you have two access points using the same channel, their Wi-Fi signals will interfere with each other.

The question states that that many users are having difficulty connecting to the company's wireless network. This is probably due to the signal being weakened by interference from another access point using the same channel. When the administrator takes a new laptop and physically goes to the access point and connects with no problems, he is able to connect because he is near the access point and therefore has a strong signal.

QUESTION NO: 557

After viewing wireless traffic, an attacker notices the following networks are being broadcasted by local access points:

Corpnet

Coffeeshop

FreePublicWifi

Using this information the attacker spoofs a response to make nearby laptops connect back to a malicious device. Which of the following has the attacker created?

- A. Infrastructure as a Service
- B. Load balancer
- C. Evil twin
- D. Virtualized network

Answer: C

Explanation:

In this question, the attacker has created another wireless network that is impersonating one of more of the three wireless networks listed in the question. This is known as an Evil Twin.

An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that

appears as a genuine hotspot offered by a legitimate provider.

In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

QUESTION NO: 558

After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output:

MACSSIDENCRYPTIONPOWERBEACONS

00:10:A1:36:12:CCMYCORPWPA2 CCMP601202

00:10:A1:49:FC:37MYCORPWPA2 CCMP709102

FB:90:11:42:FA:99MYCORPWPA2 CCMP403031

00:10:A1:AA:BB:CCMYCORPWPA2 CCMP552021

00:10:A1:FA:B1:07MYCORPWPA2 CCMP306044

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

- A. Evil twin
- B. IV attack
- C. Rogue AP
- D. DDoS

Answer: A

Explanation:

The question states that the corporate wireless network has been standardized. By 'standardized' it means the wireless network access points are running on hardware from the same vendor. We can see this from the MAC addresses used. The first half of a MAC address is vendor specific.

The second half is network adapter specific. We have four devices with MAC addresses that start with 00:10:A1.

The “odd one out” is the device with a MAC address starting FB:90:11. This device is from a different vendor. The SSID of the wireless network on this access point is the same as the other legitimate access points. Therefore, the access point with a MAC address starting FB:90:11 is impersonating the corporate access points. This is known as an Evil Twin.

An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider.

In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

QUESTION NO: 559

Which of the following types of wireless attacks would be used specifically to impersonate another WAP in order to gain unauthorized information from mobile users?

- A. IV attack
- B. Evil twin
- C. War driving
- D. Rogue access point

Answer: B

Explanation:

An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider.

In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency and SSID. To end users, the rogue evil twin appears

as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy for novice users to set up evil twin exploits.

QUESTION NO: 560

Matt, an administrator, is concerned about the wireless network being discovered by war driving.

Which of the following can be done to mitigate this?

- A.** Enforce a policy for all users to authentic through a biometric device.
- B.** Disable all SSID broadcasting.
- C.** Ensure all access points are running the latest firmware.
- D.** Move all access points into public access areas.

Answer: B

Explanation:

B: War driving is the act of using a detection tool to look for wireless networking signals. The setting making a wireless network closed (or at least hidden) is the disabling of service set identifier (SSID) broadcasting. Thus by disabling all SSID broadcasting you can mitigate the risk of war driving.

QUESTION NO: 561

Which of the following describes how Sara, an attacker, can send unwanted advertisements to a mobile device?

- A.** Man-in-the-middle
- B.** Bluejacking
- C.** Bluesnarfing
- D.** Packet sniffing

Answer: B

Explanation:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device

via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

QUESTION NO: 562

Joe, an employee is taking a taxi through a busy city and starts to receive unsolicited files sent to his Smartphone. Which of the following is this an example of?

- A. Vishing
- B. Bluejacking
- C. War Driving
- D. SPIM
- E. Bluesnarfing

Answer: B

Explanation:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

QUESTION NO: 563

A user commuting to work via public transport received an offensive image on their smart phone from another commuter. Which of the following attacks MOST likely took place?

- A. War chalking
- B. Bluejacking

- C. War driving
- D. Bluesnarfing

Answer: B

Explanation:

The question states that the 'attack' took place on public transport and was received on a smartphone. Therefore, it is most likely that the image was sent using Bluetooth.

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

QUESTION NO: 564

Which of the following is characterized by an attack against a mobile device?

- A. Evil twin
- B. Header manipulation
- C. Blue jacking
- D. Rogue AP

Answer: C

Explanation:

A bluejacking attack is where unsolicited messages are sent to mobile devices using Bluetooth. Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

QUESTION NO: 565

Which of the following attacks allows access to contact lists on cellular phones?

- A. War chalking
- B. Blue jacking
- C. Packet sniffing
- D. Bluesnarfing

Answer: D

Explanation:

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages -- without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled.

QUESTION NO: 566

An administrator has advised against the use of Bluetooth phones due to bluesnarfing concerns.

Which of the following is an example of this threat?

- A. An attacker using the phone remotely for spoofing other phone numbers
- B. Unauthorized intrusions into the phone to access data
- C. The Bluetooth enabled phone causing signal interference with the network
- D. An attacker using exploits that allow the phone to be disabled

Answer: B

Explanation:

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluetooth is a high-speed but very short-range wireless technology for exchanging data between desktop and mobile computers, personal digital assistants (PDAs), and other devices. By exploiting a vulnerability in the way Bluetooth is implemented on a mobile phone, an attacker can access information -- such as the user's calendar, contact list and e-mail and text messages --

without leaving any evidence of the attack. Other devices that use Bluetooth, such as laptop computers, may also be vulnerable, although to a lesser extent, by virtue of their more complex systems. Operating in invisible mode protects some devices, but others are vulnerable as long as Bluetooth is enabled.

QUESTION NO: 567

After a user performed a war driving attack, the network administrator noticed several similar markings where WiFi was available throughout the enterprise. Which of the following is the term used to describe these markings?

- A. IV attack
- B. War dialing
- C. Rogue access points
- D. War chalking

Answer: D

Explanation:

War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

QUESTION NO: 568

The practice of marking open wireless access points is called which of the following?

- A. War dialing
- B. War chalking
- C. War driving
- D. Evil twin

Answer: B

Explanation:

War chalking is the act of making chalk marks on outdoor surfaces (walls, sidewalks, buildings, sign posts, trees) to indicate the existence of an open wireless network connection, usually offering an Internet connection so that others can benefit from the free wireless access. The open

connections typically come from the access points of wireless networks located within buildings to serve enterprises. The chalk symbols indicate the type of access point that is available at that specific spot.

QUESTION NO: 569

Which of the following types of attacks involves interception of authentication traffic in an attempt to gain unauthorized access to a wireless network?

- A. Near field communication
- B. IV attack
- C. Evil twin
- D. Replay attack

Answer: B

Explanation:

An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session.

An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack.

A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "l" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "l" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.

Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance.

WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

QUESTION NO: 570

Sara, a security administrator, is noticing a slow down in the wireless network response. Sara launches a wireless sniffer and sees a large number of ARP packets being sent to the AP. Which of the following type of attacks is underway?

- A. IV attack
- B. Interference
- C. Blue jacking
- D. Packet sniffing

Answer: A

Explanation:

In this question, it's likely that someone is trying to crack the wireless network security.

An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per session.

An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV attack.

A particular binary sequence may be repeated more than once in a message, and the more it appears, the more the encryption method is discoverable. For example if a one-letter word exists in a message, it may be either "a" or "l" but it can't be "e" because the word "e" is non-sensical in English, while "a" has a meaning and "l" has a meaning. Repeating the words and letters makes it possible for software to apply a dictionary and discover the binary sequence corresponding to each letter.

Using an initialization vector changes the binary sequence corresponding to each letter, enabling the letter "a" to be represented by a particular sequence in the first instance, and then represented by a completely different binary sequence in the second instance.

WEP (Wireless Equivalent Privacy) is vulnerable to an IV attack. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

QUESTION NO: 571

Maintenance workers find an active network switch hidden above a dropped-ceiling tile in the CEO's office with various connected cables from the office. Which of the following describes the type of attack that was occurring?

- A. Spear phishing
- B. Packet sniffing
- C. Impersonation
- D. MAC flooding

Answer: B

Explanation:

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing. However, packet sniffing requires a physical connection to the network. The switch hidden in the ceiling is used to provide the physical connection to the network.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

QUESTION NO: 572

Which statement is TRUE about the operation of a packet sniffer?

- A. It can only have one interface on a management network.
- B. They are required for firewall operation and stateful inspection.
- C. The Ethernet card must be placed in promiscuous mode.
- D. It must be placed on a single virtual LAN interface.

Answer: C

Explanation:

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the

case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

QUESTION NO: 573

Which of the following network devices is used to analyze traffic between various network interfaces?

- A. Proxies
- B. Firewalls
- C. Content inspection
- D. Sniffers

Answer: D

Explanation:

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

QUESTION NO: 574

Which of the following software allows a network administrator to inspect the protocol header in order to troubleshoot network issues?

- A. URL filter
- B. Spam filter
- C. Packet sniffer
- D. Switch

Answer: C

Explanation:

Every data packet transmitted across a network has a protocol header. To view a protocol header, you need to capture and view the contents of the packet with a packet sniffer.

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

QUESTION NO: 575

A security administrator discovered that all communication over the company's encrypted wireless network is being captured by savvy employees with a wireless sniffing tool and is then being decrypted in an attempt to steal other employee's credentials. Which of the following technology is MOST likely in use on the company's wireless?

- A. WPA with TKIP
- B. VPN over open wireless
- C. WEP128-PSK
- D. WPA2-Enterprise

Answer: C

Explanation:

WEP's major weakness is its use of static encryption keys. When you set up a router with a WEP encryption key, that one key is used by every device on your network to encrypt every packet that's transmitted. But the fact that packets are encrypted doesn't prevent them from being intercepted, and due to some esoteric technical flaws it's entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is.

This problem used to be something you could mitigate by periodically changing the WEP key (which is why routers generally allow you to store up to four keys). But few bother to do this because changing WEP keys is inconvenient and time-consuming because it has to be done not just on the router, but on every device that connects to it. As a result, most people just set up a single key and then continue using it ad infinitum.

Even worse, for those that do change the WEP key, new research and developments reinforce how even changing WEP keys frequently is no longer sufficient to protect a WLAN. The process of 'cracking' a WEP key used to require that a malicious hacker intercept millions of packets plus spend a fair amount of time and computing power. Researchers in the computer science department of a German university recently demonstrated the capability to compromise a WEP-protected network very quickly. After spending less than a minute intercepting data (fewer than 100,000 packets in all) they were able to compromise a WEP key in just three seconds.

QUESTION NO: 576

Which of the following protocols is vulnerable to man-in-the-middle attacks by NOT using end to end TLS encryption?

- A. HTTPS
- B. WEP
- C. WPA
- D. WPA 2

Answer: B

Explanation:

WEP offers no end-to-end TLS encryption.

The WEP process consists of a series of steps as follows:

The wireless client sends an authentication request.

The Access Point (AP) sends an authentication response containing clear-text (uh-oh!) challenge text.

The client takes the challenge text received and encrypts it using a static WEP key.

The client sends the encrypted authentication packet to the AP.

The AP encrypts the challenge text using its own static WEP key and compares the result to the authentication packet sent by the client. If the results match, the AP begins the association process for the wireless client.

The big issue with WEP is the fact that it is very susceptible to a Man in the Middle attack. The attacker captures the clear-text challenge and then the authentication packet reply. The attacker then reverses the RC4 encryption in order to derive the static WEP key. Yikes!

As you might guess, the designers attempted to strengthen WEP using the approach of key lengths. The native Windows client supported a 104-bit key as opposed to the initial 40-bit key. The fundamental weaknesses in the WEP process still remained however.

QUESTION NO: 577

Which of the following wireless protocols could be vulnerable to a brute-force password attack? (Select TWO).

- A. WPA2-PSK
- B. WPA - EAP - TLS
- C. WPA2-CCMP
- D. WPA -CCMP
- E. WPA - LEAP
- F. WEP

Answer: A,E

Explanation:

A brute force attack is an attack that attempts to guess a password. WPA2-PSK and WEP both use a "Pre-Shared Key". The pre-shared key is a password and therefore is susceptible to a brute force attack.

QUESTION NO: 578

A victim is logged onto a popular home router forum site in order to troubleshoot some router configuration issues. The router is a fairly standard configuration and has an IP address of

192.168.1.1. The victim is logged into their router administrative interface in one tab and clicks a forum link in another tab. Due to clicking the forum link, the home router reboots. Which of the following attacks MOST likely occurred?

- A. Brute force password attack
- B. Cross-site request forgery
- C. Cross-site scripting
- D. Fuzzing

Answer: B

Explanation:

Cross-Site Request Forgery—also known as XSRF, session riding, and one-click attack—involves unauthorized commands coming from a trusted user to the website. This is often done without the user's knowledge, and it employs some type of social networking to pull it off. For example, assume that Evan and Spencer are chatting through Facebook. Spencer sends Evan a link to what he purports is a funny video that will crack him up. Evan clicks the link, but it actually brings up Evan's bank account information in another browser tab, takes a screenshot of it, closes the tab, and sends the information to Spencer. The reason the attack is possible is because Evan is a trusted user with his own bank. In order for it to work, Evan would need to have recently accessed

that bank's website and have a cookie that had yet to expire. The best protection against cross-site scripting is to disable the running of scripts (and browser profiles).

QUESTION NO: 579

A security administrator develops a web page and limits input into the fields on the web page as well as filters special characters in output. The administrator is trying to prevent which of the following attacks?

- A. Spoofing
- B. XSS
- C. Fuzzing
- D. Pharming

Answer: B

Explanation:

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

By validating user input and preventing special characters, we can prevent the injection of client-side scripting code.

QUESTION NO: 580

Pete, the security administrator, has been notified by the IDS that the company website is under attack. Analysis of the web logs show the following string, indicating a user is trying to post a comment on the public bulletin board.

INSERT INTO message `<script>source=http://evilsite</script>

This is an example of which of the following?

- A. XSS attack
- B. XML injection attack
- C. Buffer overflow attack
- D. SQL injection attack

Answer: A

Explanation:

The <script> </script> tags indicate that script is being inserted.

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users.

Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access-privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

QUESTION NO: 581

Which of the following BEST describes a protective countermeasure for SQL injection?

- A. Eliminating cross-site scripting vulnerabilities
- B. Installing an IDS to monitor network traffic
- C. Validating user input in web applications
- D. Placing a firewall between the Internet and database servers

Answer: C

Explanation:

By validating user input and preventing special characters, we can prevent the injection of client-side scripting code.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 582

A security administrator looking through IDS logs notices the following entry: (where email=joe@joe.com and passwd= 'or 1==1')

Which of the following attacks had the administrator discovered?

- A. SQL injection
- B. XML injection
- C. Cross-site script
- D. Header manipulation

Answer: A

Explanation:

The code in the question is an example of a SQL Injection attack. The code '1==1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 583

Which of the following types of application attacks would be used to specifically gain unauthorized information from databases that did not have any input validation implemented?

- A. SQL injection
- B. Session hijacking and XML injection
- C. Cookies and attachments
- D. Buffer overflow and XSS

Answer: A

Explanation:

To access information in databases, you use SQL. To gain unauthorized information from databases, a SQL Injection attack is used.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 584

The string:

' or 1=1-- -

Represents which of the following?

- A. Bluejacking
- B. Rogue access point
- C. SQL Injection
- D. Client-side attacks

Answer: C

Explanation:

The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 585

When an order was submitted via the corporate website, an administrator noted special characters

(e.g., ";" and "or 1=1 --") were input instead of the expected letters and numbers.

Which of the following is the MOST likely reason for the unusual results?

- A. The user is attempting to hijack the web server session using an open-source browser.
- B. The user has been compromised by a cross-site scripting attack (XSS) and is part of a botnet performing DDoS attacks.
- C. The user is attempting to fuzz the web server by entering foreign language characters which are incompatible with the website.
- D. The user is sending malicious SQL injection strings in order to extract sensitive company or customer data via the website.

Answer: D

Explanation:

The code in the question is an example of a SQL Injection attack. The code '1=1' will always provide a value of true. This can be included in statement designed to return all rows in a SQL table.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 586

Highly sensitive data is stored in a database and is accessed by an application on a DMZ server. The disk drives on all servers are fully encrypted. Communication between the application server and end-users is also encrypted. Network ACLs prevent any connections to the database server except from the application server. Which of the following can still result in exposure of the sensitive data in the database server?

- A. SQL Injection
- B. Theft of the physical database server
- C. Cookies
- D. Cross-site scripting

Answer: A

Explanation:

The question discusses a very secure environment with disk and transport level encryption and access control lists restricting access. SQL data in a database is accessed by SQL queries from an application on the application server. The data can still be compromised by a SQL injection attack.

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 587

Which of the following BEST describes a SQL Injection attack?

- A.** The attacker attempts to have the receiving server pass information to a back-end database from which it can compromise the stored information.
- B.** The attacker attempts to have the receiving server run a payload using programming commonly found on web servers.
- C.** The attacker overwhelms a system or application, causing it to crash and bring the server down to cause an outage.
- D.** The attacker overwhelms a system or application, causing it to crash, and then redirects the memory address to read from a location holding the payload.

Answer: A

Explanation:

SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

QUESTION NO: 588

An attacker attempted to compromise a web form by inserting the following input into the username field: admin)|((password=*))

Which of the following types of attacks was attempted?

- A. SQL injection
- B. Cross-site scripting
- C. Command injection
- D. LDAP injection

Answer: D

Explanation:

LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements using a local proxy. This could result in the execution of arbitrary commands such as granting permissions to unauthorized queries, and content modification inside the LDAP tree. The same advanced exploitation techniques available in SQL Injection can be similarly applied in LDAP Injection.

In a page with a user search form, the following code is responsible to catch input value and generate a LDAP query that will be used in LDAP database.

```
<input type="text" size=20 name="userName">Insert the username</input>
```

The LDAP query is narrowed down for performance and the underlying code for this function might be the following:

```
String ldapSearchQuery = "(cn=" + $userName + ")";  
System.out.println(ldapSearchQuery);
```

If the variable \$userName is not validated, it could be possible accomplish LDAP injection, as follows:

If a user puts "*" on box search, the system may return all the usernames on the LDAP base
If a user puts "jonys) (| (password = *))", it will generate the code bellow revealing jonys' password (cn = jonys) (| (password = *))

QUESTION NO: 589

Which of the following application attacks is used against a corporate directory service where there are unknown servers on the network?

- A. Rogue access point
- B. Zero day attack
- C. Packet sniffing
- D. LDAP injection

Answer: D

Explanation: A directory service is accessed by using LDAP (Lightweight Directory Access

Protocol). LDAP injection is an attack against a directory service.

Just as SQL injection attacks take statements that are input by users and exploit weaknesses within, an LDAP injection attack exploits weaknesses in LDAP (Lightweight Directory Access Protocol) implementations. This can occur when the user's input is not properly filtered, and the result can be executed commands, modified content, or results returned to unauthorized queries. The best way to prevent LDAP injection attacks is to filter the user input and to use a validation scheme to make certain that queries do not contain exploits.

One of the most common uses of LDAP is associated with user information. Numerous applications exist—such as employee directories—where users find other users by typing in a portion of their name. These queries are looking at the cn value or other fields (those defined for department, home directory, and so on). Someone attempting LDAP injection could feed unexpected values to the query to see what results are returned. All too often, finding employee information equates to finding usernames and values about those users that could be portions of their passwords.

QUESTION NO: 590

Sara, a hacker, is completing a website form to request a free coupon. The site has a field that limits the request to 3 or fewer coupons. While submitting the form, Sara runs an application on her machine to intercept the HTTP POST command and change the field from 3 coupons to 30.

Which of the following was used to perform this attack?

- A. SQL injection
- B. XML injection
- C. Packet sniffer
- D. Proxy

Answer: B

Explanation:

When a web user takes advantage of a weakness with SQL by entering values that they should not, it is known as a SQL injection attack. Similarly, when the user enters values that query XML (known as XPath) with values that take advantage of exploits, it is known as an XML injection attack. XPath works in a similar manner to SQL, except that it does not have the same levels of access control, and taking advantage of weaknesses within can return entire documents. The best way to prevent XML injection attacks is to filter the user's input and sanitize it to make certain that it does not cause XPath to return more data than it should.

QUESTION NO: 591

A malicious individual is attempting to write too much data to an application's memory. Which of the following describes this type of attack?

- A. Zero-day
- B. SQL injection
- C. Buffer overflow
- D. XSRF

Answer: C

Explanation:

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 592

Data execution prevention is a feature in most operating systems intended to protect against which type of attack?

- A. Cross-site scripting
- B. Buffer overflow
- C. Header manipulation
- D. SQL injection

Answer: B

Explanation:

Data Execution Prevention (DEP) is a security feature included in modern operating systems. It marks areas of memory as either "executable" or "nonexecutable", and allows only data in an "executable" area to be run by programs, services, device drivers, etc. It is known to be available in Linux, OS X, Microsoft Windows, iOS and Android operating systems.

DEP protects against some program errors, and helps prevent certain malicious exploits, especially attacks that store executable instructions in a data area via a buffer overflow.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 593

Which of the following application attacks is used to gain access to SEH?

- A. Cookie stealing
- B. Buffer overflow
- C. Directory traversal
- D. XML injection

Answer: B

Explanation:

Buffer overflow protection is used to detect the most common buffer overflows by checking that the stack has not been altered when a function returns. If it has been altered, the program exits with a segmentation fault. Microsoft's implementation of Data Execution Prevention (DEP) mode explicitly protects the pointer to the Structured Exception Handler (SEH) from being overwritten. A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 594

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

- A. Cross-site scripting
- B. Buffer overflow
- C. Header manipulation
- D. Directory traversal

Answer: B

Explanation:

When the user opens an attachment, the attachment is loaded into memory. The error is caused by a memory issue due to a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 595

A server administrator notes that a legacy application often stops running due to a memory error. When reviewing the debugging logs, they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describe?

- A. Zero-day
- B. Buffer overflow
- C. Cross site scripting
- D. Malicious add-on

Answer: B

Explanation:

This question describes a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 596

Which of the following was launched against a company based on the following IDS log?

122.41.15.252 - - [21/May/2012:00:17:20 +1200] "GET

/index.php?username=AA
A

AAA HTTP/1.1" 200 2731 "http://www.company.com/cgi-bin/

forum/commentary.pl/noframes/read/209" "Mozilla/4.0 (compatible;

MSIE 6.0; Windows NT 5.1; Hotbar 4.4.7.0)"

- A. SQL injection
- B. Buffer overflow attack
- C. XSS attack
- D. Online password crack

Answer: B

Explanation:

The username should be just a username; instead we can see it's a long line of text with an HTTP command in it. This is an example of a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger

specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 597

A security administrator examines a network session to a compromised database server with a packet analyzer. Within the session there is a repeated series of the hex character 90 (x90).

Which of the following attack types has occurred?

- A. Buffer overflow
- B. Cross-site scripting
- C. XML injection
- D. SQL injection

Answer: A

Explanation: Explanation

The hex character 90 (x90) means NOP or No Op or No Operation. In a buffer overflow attack, the buffer can be filled and overflowed with No Op commands.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 598

A security analyst, Ann, is reviewing an IRC channel and notices that a malicious exploit has been created for a frequently used application. She notifies the software vendor and asks them for remediation steps, but is alarmed to find that no patches are available to mitigate this vulnerability.

Which of the following BEST describes this exploit?

- A. Malicious insider threat
- B. Zero-day
- C. Client-side attack
- D. Malicious add-on

Answer: B

Explanation:

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

In this question, there are no patches available to mitigate the vulnerability. This is therefore a zero-day vulnerability.

QUESTION NO: 599

Using a heuristic system to detect an anomaly in a computer’s baseline, a system administrator was able to detect an attack even though the company signature based IDS and antivirus did not detect it. Further analysis revealed that the attacker had downloaded an executable file onto the company PC from the USB port, and executed it to trigger a privilege escalation flaw.

Which of the following attacks has MOST likely occurred?

- A. Cookie stealing
- B. Zero-day
- C. Directory traversal
- D. XML injection

Answer: B

Explanation:

The vulnerability was unknown in that the IDS and antivirus did not detect it. This is zero day vulnerability.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the

vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 600

An attacker used an undocumented and unknown application exploit to gain access to a file server. Which of the following BEST describes this type of attack?

- A. Integer overflow
- B. Cross-site scripting
- C. Zero-day
- D. Session hijacking
- E. XML injection

Answer: C

Explanation:

The vulnerability is undocumented and unknown. This is zero day vulnerability.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 601

Which of the following can only be mitigated through the use of technical controls rather than user security training?

- A. Shoulder surfing
- B. Zero-day
- C. Vishing
- D. Trojans

Answer: B

Explanation:

A zero day vulnerability is an unknown vulnerability in a software application. This cannot be prevented by user security training.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this

exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 602

The security administrator is observing unusual network behavior from a workstation. The workstation is communicating with a known malicious destination over an encrypted tunnel. A full antivirus scan, with an updated antivirus definition file, does not show any signs of infection.

Which of the following has happened on the workstation?

- A. Zero-day attack
- B. Known malware infection
- C. Session hijacking
- D. Cookie stealing

Answer: A

Explanation:

The vulnerability was unknown in that the full antivirus scan did not detect it. This is zero day vulnerability.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 603

Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?

- A. Zero-day
- B. LDAP injection
- C. XML injection
- D. Directory traversal

Answer: A

Explanation:

The security breaches have NOT yet been identified. This is zero day vulnerability.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 604

Which of the following may cause Jane, the security administrator, to seek an ACL work around?

- A. Zero day exploit
- B. Dumpster diving
- C. Virus outbreak
- D. Tailgating

Answer: A

Explanation:

A zero day vulnerability is an unknown vulnerability so there is no fix or patch for it. One way to attempt to work around a zero day vulnerability would be to restrict the permissions by using an ACL (Access Control List)

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term “zero day” refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 605

Matt, an IT administrator, wants to protect a newly built server from zero day attacks. Which of the following would provide the BEST level of protection?

- A. HIPS
- B. Antivirus
- C. NIDS
- D. ACL

Answer: A

Explanation:

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and/or system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host.

A Host-based intrusion prevention system (HIPS) is an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. As a zero-day attack is an unknown vulnerability (a vulnerability that does not have a fix or a patch to prevent it), the best defence would be an intrusion prevention system.

QUESTION NO: 606

Joe, a user, in a coffee shop is checking his email over a wireless network. An attacker records the temporary credentials being passed to Joe's browser. The attacker later uses the credentials to impersonate Joe and creates SPAM messages. Which of the following attacks allows for this impersonation?

- A. XML injection
- B. Directory traversal
- C. Header manipulation
- D. Session hijacking

Answer: D

Explanation:

In computer science, session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular

relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

QUESTION NO: 607

How often, at a MINIMUM, should Sara, an administrator, review the accesses and rights of the users on her system?

- A. Annually
- B. Immediately after an employee is terminated
- C. Every five years
- D. Every time they patch the server

Answer: A

Explanation:

Reviewing the accesses and rights of the users on a system at least annually is acceptable practice. More frequently would be desirable but too frequently would be a waste of administrative time.

QUESTION NO: 608

Which of the following types of logs could provide clues that someone has been attempting to compromise the SQL Server database?

- A. Event
- B. SQL_LOG
- C. Security
- D. Access

Answer: A

Explanation:

Event logs include Application logs, such as those where SQL Server would write entries. This is where you would see logs with details of someone trying to access a SQL database.

QUESTION NO: 609

Ann, the security administrator, received a report from the security technician, that an

unauthorized new user account was added to the server over two weeks ago. Which of the following could have mitigated this event?

- A. Routine log audits
- B. Job rotation
- C. Risk likelihood assessment
- D. Separation of duties

Answer: A

Explanation:

When a new user account is created, an entry is added to the Event Logs. By routinely auditing the event logs, you would know that an account has been created.

QUESTION NO: 610

A security administrator needs to determine which system a particular user is trying to login to at various times of the day. Which of the following log types would the administrator check?

- A. Firewall
- B. Application
- C. IDS
- D. Security

Answer: D

Explanation:

The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as the creating, opening, or deleting of files. For example, when logon auditing is enabled, an event is recorded in the security log each time a user attempts to log on to the computer. You must be logged on as Administrator or as a member of the Administrators group in order to turn on, use, and specify which events are recorded in the security log.

QUESTION NO: 611

The security administrator is analyzing a user's history file on a Unix server to determine if the user was attempting to break out of a rootjail. Which of the following lines in the user's history log shows evidence that the user attempted to escape the rootjail?

- A. `cd ../../../../bin/bash`
- B. `whoami`
- C. `ls /root`

D. `sudo -u root`

Answer: A

Explanation:

On modern UNIX variants, including Linux, you can define the root directory on a perprocess basis. The `chroot` utility allows you to run a process with a root directory other than `/`.

The root directory appears at the top of the directory hierarchy and has no parent: A process cannot access any files above the root directory (because they do not exist). If, for example, you run a program (process) and specify its root directory as `/home/sam/jail`, the program would have no concept of any files in `/home/sam` or above: `jail` is the program's root directory and is labeled `/` (not `jail`).

By creating an artificial root directory, frequently called a (chroot) jail, you prevent a program from accessing or modifying—possibly maliciously—files outside the directory hierarchy starting at its root. You must set up a chroot jail properly to increase security: If you do not set up the chroot jail correctly, you can actually make it easier for a malicious user to gain access to a system than if there were no chroot jail.

The command `cd ..` takes you up one level in the directory structure. Repeated commands would take you to the top level the root which is represented by a forward slash `/`. The command `/bin/bash` is an attempt to run the bash shell from the root level.

QUESTION NO: 612

A security technician is attempting to improve the overall security posture of an internal mail server. Which of the following actions would BEST accomplish this goal?

- A. Monitoring event logs daily
- B. Disabling unnecessary services
- C. Deploying a content filter on the network
- D. Deploy an IDS on the network

Answer: B

Explanation:

One of the most basic practices for reducing the attack surface of a specific host is to disable unnecessary services. Services running on a host, especially network services provide an avenue through which the system can be attacked. If a service is not being used, disable it.

QUESTION NO: 613

A vulnerability assessment indicates that a router can be accessed from default port 80 and default port 22. Which of the following should be executed on the router to prevent access via these ports? (Select TWO).

- A. FTP service should be disabled
- B. HTTPS service should be disabled
- C. SSH service should be disabled
- D. HTTP service should disabled
- E. Telnet service should be disabled

Answer: C,D

Explanation:

Port 80 is used by HTTP. Port 22 is used by SSH. By disabling the HTTP and Telnet services, you will prevent access to the router on ports 80 and 22.

QUESTION NO: 614

During a routine audit a web server is flagged for allowing the use of weak ciphers. Which of the following should be disabled to mitigate this risk? (Select TWO).

- A. SSL 1.0
- B. RC4
- C. SSL 3.0
- D. AES
- E. DES
- F. TLS 1.0

Answer: A,E

Explanation:

TLS 1.0 and SSL 1.0 both have known vulnerabilities and have been replaced by later versions. Any systems running these ciphers should have them disabled.

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product, message authentication Netscape developed the original SSL protocol. Version 1.0 was never publicly released because of serious security flaws in the protocol; version 2.0, released in February 1995, "contained a number of security flaws which ultimately led to the design of SSL version 3.0".

TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As

stated in the RFC, "the differences between this protocol and SSL 3.0 are not dramatic, but they are significant enough to preclude interoperability between TLS 1.0 and SSL 3.0". TLS 1.0 does include a means by which a TLS implementation can downgrade the connection to SSL 3.0, thus weakening security.

TLS 1.1 and then TLS 1.2 were created to replace TLS 1.0.

QUESTION NO: 615

A new web server has been provisioned at a third party hosting provider for processing credit card transactions. The security administrator runs the netstat command on the server and notices that ports 80, 443, and 3389 are in a 'listening' state. No other ports are open. Which of the following services should be disabled to ensure secure communications?

- A. HTTPS
- B. HTTP
- C. RDP
- D. TELNET

Answer: B

Explanation:

HTTP uses port 80. HTTP does not provide encrypted communications. Port 443 is used by HTTPS which provides secure encrypted communications. Port 3389 is used by RDP (Remote Desktop Protocol) which does provide encrypted communications.

QUESTION NO: 616

Joe analyzed the following log and determined the security team should implement which of the following as a mitigation method against further attempts?

Host 192.168.1.123

[00: 00: 01]Successful Login: 015 192.168.1.123 : local

[00: 00: 03]Unsuccessful Login: 022 214.34.56.006 : RDP 192.168.1.124

[00: 00: 04]UnSuccessful Login: 010 214.34.56.006 : RDP 192.168.1.124

[00: 00: 07]UnSuccessful Login: 007 214.34.56.006 : RDP 192.168.1.124

[00: 00: 08]UnSuccessful Login: 003 214.34.56.006 : RDP 192.168.1.124

- A. Reporting
- B. IDS
- C. Monitor system logs
- D. Hardening

Answer: D

Explanation:

We can see a number of unsuccessful login attempts using a Remote Desktop Connection (using the RDP protocol) from a computer with the IP address 192.168.1.124.

Someone successfully logged in locally. This is probably an authorized login (for example, Joe logging in).

Hardening is the process of securing a system. We can harden (secure) the system by either disallowing remote desktop connections altogether or by restricting which IPs are allowed to initiate remote desktop connections.

QUESTION NO: 617

The Chief Technology Officer (CTO) wants to improve security surrounding storage of customer passwords.

The company currently stores passwords as SHA hashes. Which of the following can the CTO implement requiring the LEAST change to existing systems?

- A. Smart cards
- B. TOTP
- C. Key stretching
- D. Asymmetric keys

Answer: A

Explanation:

Smart cards usually come in two forms. The most common takes the form of a rectangular piece of plastic with an embedded microchip. The second is as a USB token. It contains a built in processor and has the ability to securely store and process information. A "contact" smart card communicates with a PC using a smart card reader whereas a "contactless" card sends encrypted information via radio waves to the PC.

Typical scenarios in which smart cards are used include interactive logon, e-mail signing, e-mail decryption and remote access authentication. However, smart cards are programmable and can contain programs and data for many different applications. For example smart cards may be used to store medical histories for use in emergencies, to make electronic cash payments or to verify the identity of a customer to an e-retailer.

Microsoft provides two device independent APIs to insulate application developers from

differences between current and future implementations: CryptoAPI and Microsoft Win32® SCard APIs.

The Cryptography API contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs).

There are many different cryptographic algorithms and even when implementing the same algorithm there are many choices to make about key sizes and padding for example. For this reason, CSPs are grouped into types, in which each supported CryptoAPI function, by default, performs in a way particular to that type. For example, CSPs in the PROV_DSS provider type support DSS Signatures and MD5 and SHA hashing.

QUESTION NO: 618

An auditor's report discovered several accounts with no activity for over 60 days. The accounts were later identified as contractors' accounts who would be returning in three months and would need to resume the activities. Which of the following would mitigate and secure the auditors finding?

- A. Disable unnecessary contractor accounts and inform the auditor of the update.
- B. Reset contractor accounts and inform the auditor of the update.
- C. Inform the auditor that the accounts belong to the contractors.
- D. Delete contractor accounts and inform the auditor of the update.

Answer: A

Explanation:

A disabled account cannot be used. It is 'disabled'. Whenever an employee leaves a company, the employee's user account should be disabled. The question states that the accounts are contractors' accounts who would be returning in three months. Therefore, it would be easier to keep the accounts rather than deleting them which would require that the accounts are recreated in three months time. By disabling the accounts, we can ensure that the accounts cannot be used; in three months when the contractors are back, we can simply re-enable the accounts.

QUESTION NO: 619

An administrator notices that former temporary employees' accounts are still active on a domain. Which of the following can be implemented to increase security and prevent this from happening?

- A. Implement a password expiration policy.
- B. Implement an account expiration date for permanent employees.
- C. Implement time of day restrictions for all temporary employees.
- D. Run a last logon script to look for inactive accounts.

Answer: D

Explanation:

You can run a script to return a list of all accounts that haven't been used for a number of days, for example 30 days. If an account hasn't been logged into for 30 days, it's a safe bet that the user the account belonged to is no longer with the company. You can then disable all the accounts that the script returns. A disabled account cannot be used to log in to a system. This is a good security measure. As soon as an employee leaves the company, the employees account should always be disabled.

QUESTION NO: 620

How must user accounts for exiting employees be handled?

- A. Disabled, regardless of the circumstances
- B. Disabled if the employee has been terminated
- C. Deleted, regardless of the circumstances
- D. Deleted if the employee has been terminated

Answer: A

Explanation:

You should always disable an employee's account as soon as they leave. The employee knows the username and password of the account and could continue to log in for potentially malicious purposes. Disabling the account will ensure that no one can log in using that account.

QUESTION NO: 621

An administrator has a network subnet dedicated to a group of users. Due to concerns regarding data and network security, the administrator desires to provide network access for this group only. Which of the following would BEST address this desire?

- A. Install a proxy server between the users' computers and the switch to filter inbound network traffic.
- B. Block commonly used ports and forward them to higher and unused port numbers.
- C. Configure the switch to allow only traffic from computers based upon their physical address.
- D. Install host-based intrusion detection software to monitor incoming DHCP Discover requests.

Answer: C

Explanation:

Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter.

You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses.

MAC filtering is commonly used in wireless networks but is considered insecure because a MAC address can be spoofed. However, in a wired network, it is more secure because it would be more difficult for a rogue computer to sniff a MAC address.

QUESTION NO: 622

A new virtual server was created for the marketing department. The server was installed on an existing host machine. Users in the marketing department report that they are unable to connect to the server. Technicians verify that the server has an IP address in the same VLAN as the marketing department users. Which of the following is the MOST likely reason the users are unable to connect to the server?

- A. The new virtual server's MAC address was not added to the ACL on the switch
- B. The new virtual server's MAC address triggered a port security violation on the switch
- C. The new virtual server's MAC address triggered an implicit deny in the switch
- D. The new virtual server's MAC address was not added to the firewall rules on the switch

Answer: A

Explanation:

Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter.

You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses.

In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

QUESTION NO: 623

Which of the following can be implemented if a security administrator wants only certain devices connecting to the wireless network?

- A. Disable SSID broadcast
- B. Install a RADIUS server
- C. Enable MAC filtering
- D. Lowering power levels on the AP

Answer: C

Explanation:

MAC filtering is commonly used in wireless networks. In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

QUESTION NO: 624

Which of the following implementation steps would be appropriate for a public wireless hot-spot?

- A. Reduce power level
- B. Disable SSID broadcast
- C. Open system authentication
- D. MAC filter

Answer: C

Explanation:

For a public wireless hot-spot, you want members of the public to be able to access the wireless network without having to provide them with a password. Therefore, Open System Authentication is the best solution.

Open System Authentication (OSA) is a process by which a computer can gain access to a wireless network that uses the Wired Equivalent Privacy (WEP) protocol. With OSA, a computer equipped with a wireless modem can access any WEP network and receive files that are not encrypted.

For OSA to work, the service set identifier (SSID) of the computer should match the SSID of the

wireless access point. The SSID is a sequence of characters that uniquely names a wireless local area network (WLAN). The process occurs in three steps. First, the computer sends a request for authentication to the access point. Then the access point generates an authentication code, usually at random, intended for use only during that session. Finally, the computer accepts the authentication code and becomes part of the network as long as the session continues and the computer remains within range of the original access point.

If it is necessary to exchange encrypted data between a WEP network access point and a wireless-equipped computer, a stronger authentication process called Shared Key Authentication (SKA) is required.

QUESTION NO: 625

Which of the following controls would allow a company to reduce the exposure of sensitive systems from unmanaged devices on internal networks?

- A. 802.1x
- B. Data encryption
- C. Password strength
- D. BGP

Answer: A

Explanation:

IEEE 802.1X (also known as Dot1x) is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN - though the term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the

network.

QUESTION NO: 626

A system security analyst using an enterprise monitoring tool notices an unknown internal host exfiltrating files to several foreign IP addresses. Which of the following would be an appropriate mitigation technique?

- A. Disabling unnecessary accounts
- B. Rogue machine detection
- C. Encrypting sensitive files
- D. Implementing antivirus

Answer: B

Explanation:

Rogue machine detection is the process of detecting devices on the network that should not be there. If a user brings in a laptop and plugs it into the network, the laptop is a "rogue machine". The laptop could cause problems on the network. Any device on the network that should not be there is classed as rogue.

QUESTION NO: 627

Matt, a developer, recently attended a workshop on a new application. The developer installs the new application on a production system to test the functionality. Which of the following is MOST likely affected?

- A. Application design
- B. Application security
- C. Initial baseline configuration
- D. Management of interfaces

Answer: C

Explanation:

The initial baseline configuration of a computer system is an agreed configuration for the computer. For example, the initial baseline configuration will list what operating system the computer will run, what software applications and patches will be installed and what configuration settings should be applied to the system.

In this question, we are installing a new software application on a server. After the installation of the software, the "configuration" of the server (installed software, settings etc) is now different from

the initial baseline configuration.

QUESTION NO: 628

In order to maintain oversight of a third party service provider, the company is going to implement a Governance, Risk, and Compliance (GRC) system. This system is promising to provide overall security posture coverage. Which of the following is the MOST important activity that should be considered?

- A. Continuous security monitoring
- B. Baseline configuration and host hardening
- C. Service Level Agreement (SLA) monitoring
- D. Security alerting and trending

Answer: A

Explanation:

The company is investing in a Governance, Risk, and Compliance (GRC) system to provide overall security posture coverage. This is great for testing the security posture. However, to be effective and ensure the company always has a good security posture, you need to monitor the security continuously.

Once a baseline security configuration is documented, it is critical to monitor it to see that this baseline is maintained or exceeded. A popular phrase among personal trainers is "that which gets measured gets improved." Well, in network security, "that which gets monitored gets secure." Continuous monitoring means exactly that: ongoing monitoring. This may involve regular measurements of network traffic levels, routine evaluations for regulatory compliance, and checks of network security device configurations.

QUESTION NO: 629

A security analyst performs the following activities: monitors security logs, installs surveillance cameras and analyzes trend reports. Which of the following job responsibilities is the analyst performing? (Select TWO).

- A. Detect security incidents
- B. Reduce attack surface of systems
- C. Implement monitoring controls
- D. Hardening network devices
- E. Prevent unauthorized access

Answer: A,C

Explanation:

By monitoring security logs, installing security cameras and analyzing trend reports, the security analyst is implementing monitoring controls.

With the monitoring controls in place, by monitoring the security logs, reviewing the footage from the security cameras and analyzing trend reports, the security analyst is able to detect security incidents.

QUESTION NO: 630

Which of the following is an indication of an ongoing current problem?

- A. Alert
- B. Trend
- C. Alarm
- D. Trap

Answer: C

Explanation:

An alarm indicates that something is wrong and needs to be resolved as soon as possible. Alarms usually continue to sound until the problem is resolved or the alarm is manually silenced.

QUESTION NO: 631

Which of the following is a notification that an unusual condition exists and should be investigated?

- A. Alert
- B. Trend
- C. Alarm
- D. Trap

Answer: A

Explanation:

We need to look carefully at the wording of the question to determine the answer. This question is asking about an “unusual condition” that should be investigated. There are different levels of alerts from Critical to Warning to Information only.

An Alarm would be triggered by a serious definite problem that needs resolving urgently. An “unusual condition” probably wouldn’t trigger an alarm; it is more likely to trigger an Alert.

QUESTION NO: 632

A security manager must remain aware of the security posture of each system. Which of the following supports this requirement?

- A. Training staff on security policies
- B. Establishing baseline reporting
- C. Installing anti-malware software
- D. Disabling unnecessary accounts/services

Answer: B

Explanation:

The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.

A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

QUESTION NO: 633

Suspicious traffic without a specific signature was detected. Under further investigation, it was determined that these were false indicators. Which of the following security devices needs to be configured to disable future false alarms?

- A. Signature based IPS
- B. Signature based IDS
- C. Application based IPS
- D. Anomaly based IDS

Answer: D

Explanation:

Most intrusion detection systems (IDS) are what is known as signature-based. This means that they operate in much the same way as a virus scanner, by searching for a known identity - or signature - for each specific intrusion event. And, while signature-based IDS is very efficient at sniffing out known s of attack, it does, like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker technique. In other words, signature-based IDS is only as good as its database of stored signatures.

Any organization wanting to implement a more thorough - and hence safer - solution, should consider what we call anomaly-based IDS. By its nature, anomaly-based IDS is a rather more

complex creature. In network traffic terms, it captures all the headers of the IP packets running towards the network. From this, it filters out all known and legal traffic, including web traffic to the organization's web server, mail traffic to and from its mail server, outgoing web traffic from company employees and DNS traffic to and from its DNS server.

There are other equally obvious advantages to using anomaly-based IDS. For example, because it detects any traffic that is new or unusual, the anomaly method is particularly good at identifying sweeps and probes towards network hardware. It can, therefore, give early warnings of potential intrusions, because probes and scans are the predecessors of all attacks. And this applies equally to any new service installed on any item of hardware - for example, Telnet deployed on a network router for maintenance purposes and forgotten about when the maintenance was finished. This makes anomaly-based IDS perfect for detecting anything from port anomalies and web anomalies to mis-formed attacks, where the URL is deliberately mis-typed.

QUESTION NO: 634

Jane, a security administrator, has observed repeated attempts to break into a server. Which of the following is designed to stop an intrusion on a specific server?

- A. HIPS**
- B. NIDS**
- C. HIDS**
- D. NIPS**

Answer: A

Explanation:

This question is asking which of the following is designed to stop an intrusion on a specific server. To stop an intrusion on a specific server, you would use a HIPS (Host Intrusion Prevention System). The difference between a HIPS and other intrusion prevention systems is that a HIPS is a software intrusion prevention systems that is installed on a 'specific server'.

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

A HIPS (Host Intrusion Prevention System) is software installed on a host which monitors the host for suspicious activity by analyzing events occurring within that host with the aim of detecting and preventing intrusion.

QUESTION NO: 635

Which of the following tools will allow a technician to detect security-related TCP connection anomalies?

- A. Logical token
- B. Performance monitor
- C. Public key infrastructure
- D. Trusted platform module

Answer: B

Explanation:

Performance Monitor in a Windows system can monitor many different 'counters'. For TCP network connections, you can monitor specific TCP related counters including the following:

Connection Failures

Connections Active

Connections Established

Connections Passive

Connections Reset

Segments Received/sec

Segments Retransmitted/sec

Segments Sent/sec

Total Segments/sec

By monitoring the counters listed above, you will be able to detect security-related TCP connection anomalies.

QUESTION NO: 636

Which of the following would a security administrator implement in order to identify a problem between two systems that are not communicating properly?

- A. Protocol analyzer
- B. Baseline report
- C. Risk assessment
- D. Vulnerability scan

Answer: A

Explanation:

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent from two systems that are not communicating properly could help determine the cause of the issue.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

QUESTION NO: 637

Which of the following is BEST used to capture and analyze network traffic between hosts on the same network segment?

- A. Protocol analyzer
- B. Router
- C. Firewall
- D. HIPS

Answer: A

Explanation:

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent from two systems that are not communicating properly could help determine the cause of the issue.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

QUESTION NO: 638

Which of the following would a security administrator implement in order to identify a problem between two applications that are not communicating properly?

- A. Protocol analyzer
- B. Baseline report
- C. Risk assessment
- D. Vulnerability scan

Answer: A

Explanation:

A Protocol Analyzer is a hardware device or more commonly a software program used to capture

network data communications sent between devices on a network. Capturing and analyzing the packets sent between applications on systems that are not communicating properly could help determine the cause of the issue.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

QUESTION NO: 639

Which of the following tools would allow Ann, the security administrator, to be able to BEST quantify all traffic on her network?

- A. Honeypot
- B. Port scanner
- C. Protocol analyzer
- D. Vulnerability scanner

Answer: C

Explanation:

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. By capturing and analyzing the packets sent between the systems on the network, Ann would be able to quantify the amount of traffic on the network.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

QUESTION NO: 640

Joe, the security administrator, has determined that one of his web servers is under attack. Which of the following can help determine where the attack originated from?

- A. Capture system image
- B. Record time offset
- C. Screenshots
- D. Network sniffing

Answer: D

Explanation:

Network sniffing is the process of capturing and analyzing the packets sent between systems on the network. A network sniffer is also known as a Protocol Analyzer.

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing and analyzing the packets sent to the web server will help determine the source IP address of the system sending the packets.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

QUESTION NO: 641

Which of the following BEST allows Pete, a security administrator, to determine the type, source, and flags of the packet traversing a network for troubleshooting purposes?

- A. Switches
- B. Protocol analyzers
- C. Routers
- D. Web security gateways

Answer: B

Explanation:

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. By capturing and analyzing the packets, Pete will be able to determine the type, source, and flags of the packets traversing a network for troubleshooting purposes.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

QUESTION NO: 642

Which of the following security architecture elements also has sniffer functionality? (Select TWO).

- A. HSM
- B. IPS
- C. SSL accelerator
- D. WAP
- E. IDS

Answer: B,E

Explanation:

Sniffer functionality means the ability to capture and analyze the content of data packets as they

are transmitted across the network.

IDS and IPS systems perform their functions by capturing and analyzing the content of data packets.

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.

IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content.

QUESTION NO: 643

Which of the following would a security administrator implement in order to discover comprehensive security threats on a network?

- A. Design reviews
- B. Baseline reporting
- C. Vulnerability scan
- D. Code review

Answer: C

Explanation:

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed.

The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited

and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION NO: 644

An administrator is concerned that a company's web server has not been patched. Which of the following would be the BEST assessment for the administrator to perform?

- A.** Vulnerability scan
- B.** Risk assessment
- C.** Virus scan
- D.** Network sniffer

Answer: A

Explanation:

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. Vulnerabilities include computer systems that do not have the latest security patches installed.

The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION NO: 645

Which of the following would be used to identify the security posture of a network without actually exploiting any weaknesses?

- A. Penetration test
- B. Code review
- C. Vulnerability scan
- D. Brute Force scan

Answer: C

Explanation:

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION NO: 646

Which of the following should an administrator implement to research current attack methodologies?

- A. Design reviews
- B. Honeypot
- C. Vulnerability scanner
- D. Code reviews

Answer: B

Explanation:

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk.

Research – A research honeypot add value to research in computer security by providing a platform to study the threat.

QUESTION NO: 647

Based on information leaked to industry websites, business management is concerned that unauthorized employees are accessing critical project information for a major, well-known new product. To identify any such users, the security administrator could:

- A.** Set up a honeypot and place false project documentation on an unsecure share.
- B.** Block access to the project documentation using a firewall.
- C.** Increase antivirus coverage of the project servers.
- D.** Apply security updates and harden the OS on all project servers.

Answer: A

Explanation:

In this scenario, we would use a honeypot as a 'trap' to catch unauthorized employees who are accessing critical project information.

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk.

Research – A research honeypot add value to research in computer security by providing a platform to study the threat.

QUESTION NO: 648

Joe, an administrator, installs a web server on the Internet that performs credit card transactions for customer payments. Joe also sets up a second web server that looks like the first web server.

However, the second server contains fabricated files and folders made to look like payments were processed on this server but really were not. Which of the following is the second server?

- A. DMZ
- B. Honeynet
- C. VLAN
- D. Honeypot

Answer: D

Explanation:

In this scenario, the second web server is a 'fake' webserver designed to attract attacks. We can then monitor the second server to view the attacks and then ensure that the 'real' web server is secure against such attacks. The second web server is a honeypot.

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk.

Research – A research honeypot add value to research in computer security by providing a

platform to study the threat.

QUESTION NO: 649

Which of the following can Joe, a security administrator, implement on his network to capture attack details that are occurring while also protecting his production network?

- A. Security logs
- B. Protocol analyzer
- C. Audit logs
- D. Honeypot

Answer: D

Explanation:

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk.

Research – A research honeypot add value to research in computer security by providing a platform to study the threat.

QUESTION NO: 650

What is a system that is intended or designed to be broken into by an attacker?

- A. Honeypot
- B. Honeybucket
- C. Decoy

D. Spoofing system

Answer: A

Explanation:

A honeypot is a system whose purpose it is to be attacked. An administrator can watch and study the attack to research current attack methodologies.

According to the Wepopedia.com, a Honeypot luring a hacker into a system has several main purposes:

The administrator can watch the hacker exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned.

The hacker can be caught and stopped while trying to obtain root access to the system.

By studying the activities of hackers, designers can better create more secure systems that are potentially invulnerable to future hackers.

There are two main types of honeypots:

Production - A production honeypot is one used within an organization's environment to help mitigate risk.

Research – A research honeypot add value to research in computer security by providing a platform to study the threat.

QUESTION NO: 651

The security team would like to gather intelligence about the types of attacks being launched against the organization. Which of the following would provide them with the MOST information?

- A. Implement a honeynet
- B. Perform a penetration test
- C. Examine firewall logs
- D. Deploy an IDS

Answer: A

Explanation:

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a

non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets.

In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

A virtual honeynet is one that, while appearing to be an entire network, resides on a single server.

QUESTION NO: 652

Jane, a security analyst, is reviewing logs from hosts across the Internet which her company uses to gather data on new malware. Which of the following is being implemented by Jane's company?

- A. Vulnerability scanner
- B. Honeynet
- C. Protocol analyzer
- D. Port scanner

Answer: B

Explanation:

The Internet hosts used to gather data on new malware are known as honeypots. A collection of honeypots is known as a honeynet.

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets.

In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has

been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

A virtual honeynet is one that, while appearing to be an entire network, resides on a single server.

QUESTION NO: 653

A security administrator wants to get a real time look at what attackers are doing in the wild, hoping to lower the risk of zero-day attacks. Which of the following should be used to accomplish this goal?

- A. Penetration testing
- B. Honeynets
- C. Vulnerability scanning
- D. Baseline reporting

Answer: B

Explanation:

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets.

In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

A virtual honeynet is one that, while appearing to be an entire network, resides on a single server.

QUESTION NO: 654

During a security assessment, an administrator wishes to see which services are running on a remote server. Which of the following should the administrator use?

- A. Port scanner
- B. Network sniffer
- C. Protocol analyzer
- D. Process list

Answer: A

Explanation:

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server.

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

QUESTION NO: 655

Which of the following tools would a security administrator use in order to identify all running services throughout an organization?

- A. Architectural review
- B. Penetration test
- C. Port scanner
- D. Design review

Answer: C

Explanation:

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80

on the server. By determining which ports are open on a remote server, we can determine which services are running on that server.

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

QUESTION NO: 656

Sara, the Chief Information Officer (CIO), has requested an audit take place to determine what services and operating systems are running on the corporate network. Which of the following should be used to complete this task?

- A. Fingerprinting and password crackers
- B. Fuzzing and a port scan
- C. Vulnerability scan and fuzzing
- D. Port scan and fingerprinting

Answer: D

Explanation:

Different services use different ports. When a service is enabled on a computer, a network port is opened for that service. For example, enabling the HTTP service on a web server will open port 80 on the server. By determining which ports are open on a remote server, we can determine which services are running on that server.

A port scanner is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.

A port scan or portscan can be defined as a process that sends client requests to a range of server port addresses on a host, with the goal of finding an active port. While not a nefarious process in and of itself, it is one used by hackers to probe target machine services with the aim of exploiting a known vulnerability of that service. However the majority of uses of a port scan are not attacks and are simple probes to determine services available on a remote machine.

Fingerprinting is a means of ascertaining the operating system of a remote computer on a network. Fingerprinting is more generally used to detect specific versions of applications or

protocols that are run on network servers. Fingerprinting can be accomplished “passively” by sniffing network packets passing between hosts, or it can be accomplished “actively” by transmitting specially created packets to the target machine and analyzing the response

QUESTION NO: 657

Which device monitors network traffic in a passive manner?

- A. Sniffer
- B. IDS
- C. Firewall
- D. Web browser

Answer: A

Explanation:

A sniffer is another name for a protocol analyzer. A protocol analyzer performs its function in a passive manner. In other words, computers on the network do not know that their data packets have been captured.

A Protocol Analyzer is a hardware device or more commonly a software program used to capture network data communications sent between devices on a network. Capturing packets sent from a computer system is known as packet sniffing.

Well known software protocol analyzers include Message Analyzer (formerly Network Monitor) from Microsoft and Wireshark (formerly Ethereal).

A sniffer (packet sniffer) is a tool that intercepts data flowing in a network. If computers are connected to a local area network that is not filtered or switched, the traffic can be broadcast to all computers contained in the same segment. This doesn't generally occur, since computers are generally told to ignore all the comings and goings of traffic from other computers. However, in the case of a sniffer, all traffic is shared when the sniffer software commands the Network Interface Card (NIC) to stop ignoring the traffic. The NIC is put into promiscuous mode, and it reads communications between computers within a particular segment. This allows the sniffer to seize everything that is flowing in the network, which can lead to the unauthorized access of sensitive data. A packet sniffer can take the form of either a hardware or software solution. A sniffer is also known as a packet analyzer.

QUESTION NO: 658

A new security analyst is given the task of determining whether any of the company's servers are vulnerable to a recently discovered attack on an old version of SSH. Which of the following is the

quickest FIRST step toward determining the version of SSH running on these servers?

- A. Passive scanning
- B. Banner grabbing
- C. Protocol analysis
- D. Penetration testing

Answer: B

Explanation:

B: Banner grabbing looks at the banner, or header information messages sent with data to find out about the system(s). Banners often identify the host, the operating system running on it, and other information that can be useful if you are going to attempt to later breach the security of it. Banners can be snagged with Telnet as well as tools like netcat or Nmap. In other words Banner grabbing looks at the banner, or header, information messages sent with data to find out about the system(s). Thus a quick way to check which version of SSH is running on your server.

QUESTION NO: 659

After analyzing and correlating activity from multiple sensors, the security administrator has determined that a group of very well organized individuals from an enemy country is responsible for various attempts to breach the company network, through the use of very sophisticated and targeted attacks. Which of the following is this an example of?

- A. Privilege escalation
- B. Advanced persistent threat
- C. Malicious insider threat
- D. Spear phishing

Answer: B

Explanation:

Definitions of precisely what an APT is can vary widely, but can best be summarized by their named requirements:

Advanced – Criminal operators behind the threat utilize the full spectrum of computer intrusion technologies and techniques. While individual components of the attack may not be classed as particularly “advanced” (e.g. malware components generated from commonly available DIY construction kits, or the use of easily procured exploit materials), their operators can typically access and develop more advanced tools as required. They combine multiple attack methodologies and tools in order to reach and compromise their target.

Persistent – Criminal operators give priority to a specific task, rather than opportunistically seeking immediate financial gain. This distinction implies that the attackers are guided by external entities. The attack is conducted through continuous monitoring and interaction in order to achieve the

defined objectives. It does not mean a barrage of constant attacks and malware updates. In fact, a “low-and-slow” approach is usually more successful.

Threat – means that there is a level of coordinated human involvement in the attack, rather than a mindless and automated piece of code. The criminal operators have a specific objective and are skilled, motivated, organized and well funded.

QUESTION NO: 660

A system administrator has noticed vulnerability on a high impact production server. A recent update was made available by the vendor that addresses the vulnerability but requires a reboot of the system afterwards. Which of the following steps should the system administrator implement to address the vulnerability?

- A.** Test the update in a lab environment, schedule downtime to install the patch, install the patch and reboot the server and monitor for any changes
- B.** Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the patch, and monitor for any changes
- C.** Test the update in a lab environment, backup the server, schedule downtime to install the patch, install the update, reboot the server, and monitor for any changes
- D.** Backup the server, schedule downtime to install the patch, installs the patch and monitor for any changes

Answer: C

Explanation:

We have an update to apply to fix the vulnerability. The update should be tested first in a lab environment, not on the production server to ensure it doesn't cause any other problems with the server. After testing the update, we should backup the server to enable us to roll back any changes in the event of any unforeseen problems with the update. The question states that the server will require a reboot. This will result in downtime so you should schedule the downtime before installing the patch. After installing the update, you should monitor the server to ensure it is functioning correctly.

QUESTION NO: 661

A security specialist has been asked to evaluate a corporate network by performing a vulnerability assessment. Which of the following will MOST likely be performed?

- A.** Identify vulnerabilities, check applicability of vulnerabilities by passively testing security controls.

- B. Verify vulnerabilities exist, bypass security controls and exploit the vulnerabilities.
- C. Exploit security controls to determine vulnerabilities and misconfigurations.
- D. Bypass security controls and identify applicability of vulnerabilities by passively testing security controls.

Answer: A

Explanation:

We need to determine if vulnerabilities exist by passively testing security controls.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION NO: 662

Which of the following would a security administrator implement in order to identify change from the standard configuration on a server?

- A. Penetration test
- B. Code review
- C. Baseline review
- D. Design review

Answer: C

Explanation:

The standard configuration on a server is known as the baseline.

The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.

A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

QUESTION NO: 663

Several users report to the administrator that they are having issues downloading files from the file server. Which of the following assessment tools can be used to determine if there is an issue with the file server?

- A. MAC filter list
- B. Recovery agent
- C. Baselines
- D. Access list

Answer: C

Explanation:

The standard configuration on a server is known as the baseline. In this question, we can see if anything has changed on the file server by comparing its current configuration with the baseline. The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.

A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

QUESTION NO: 664

One of the servers on the network stops responding due to lack of available memory. Server administrators did not have a clear definition of what action should have taken place based on the available memory. Which of the following would have BEST kept this incident from occurring?

- A. Set up a protocol analyzer
- B. Set up a performance baseline
- C. Review the systems monitor on a monthly basis
- D. Review the performance monitor on a monthly basis

Answer: B

Explanation:

A performance baseline provides the input needed to design, implement, and support a secure network. The performance baseline would define the actions that should be performed on a server that is running low on memory.

QUESTION NO: 665

Ann, the software security engineer, works for a major software vendor. Which of the following

practices should be implemented to help prevent race conditions, buffer overflows, and other similar vulnerabilities prior to each production release?

- A. Product baseline report
- B. Input validation
- C. Patch regression testing
- D. Code review

Answer: D

Explanation:

The problems listed in this question can be caused by problems with the application code. Reviewing the code will help to prevent the problems.

The purpose of code review is to look at all custom written code for holes that may exist. The review needs also to examine changes that the code—most likely in the form of a finished application—may make: configuration files, libraries, and the like. During this examination, look for threats such as opportunities for injection to occur (SQL, LDAP, code, and so on), cross-site request forgery, and authentication. Code review is often conducted as a part of gray box testing. Looking at source code can often be one of the easiest ways to find weaknesses within the application. Simply reading the code is known as manual assessment, whereas using tools to scan the code is known as automated assessment.

QUESTION NO: 666

Which of the following assessment techniques would a security administrator implement to ensure that systems and software are developed properly?

- A. Baseline reporting
- B. Input validation
- C. Determine attack surface
- D. Design reviews

Answer: D

Explanation:

When implementing systems and software, an important step is the design of the systems and software. The systems and software should be designed to ensure that the system works as intended and is secure.

The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the system or application. A design review is basically a check to ensure that the design of the system meets the security requirements.

QUESTION NO: 667

A financial company requires a new private network link with a business partner to cater for realtime and batched data flows.

Which of the following activities should be performed by the IT security staff member prior to establishing the link?

- A. Baseline reporting
- B. Design review
- C. Code review
- D. SLA reporting

Answer: B

Explanation:

This question is asking about a new private network link (a VPN) with a business partner. This will provide access to the local network from the business partner.

When implementing a VPN, an important step is the design of the VPN. The VPN should be designed to ensure that the security of the network and local systems is not compromised.

The design review assessment examines the ports and protocols used, the rules, segmentation, and access control in the systems or applications. A design review is basically a check to ensure that the design of the system meets the security requirements.

QUESTION NO: 668

Which of the following assessments would Pete, the security administrator, use to actively test that an application's security controls are in place?

- A. Code review
- B. Penetration test
- C. Protocol analyzer
- D. Vulnerability scan

Answer: B

Explanation:

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting

back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

QUESTION NO: 669

Which of the following is the MOST intrusive type of testing against a production system?

- A. White box testing
- B. War dialing
- C. Vulnerability testing
- D. Penetration testing

Answer: D

Explanation:

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system.

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable

amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

QUESTION NO: 670

During an anonymous penetration test, Jane, a system administrator, was able to identify a shared print spool directory, and was able to download a document from the spool. Which statement BEST describes her privileges?

- A. All users have write access to the directory.
- B. Jane has read access to the file.
- C. All users have read access to the file.
- D. Jane has read access to the directory.

Answer: C

Explanation:

The question states that Jane was able to download a document from the spool directory. To view and download the document, Jane must have at least Read access to the file. The fact that the document belonged to someone else suggests that all users have read access to the file.

QUESTION NO: 671

During a penetration test from the Internet, Jane, the system administrator, was able to establish a connection to an internal router, but not successfully log in to it. Which ports and protocols are MOST likely to be open on the firewall? (Select FOUR).

- A. 21
- B. 22
- C. 23
- D. 69
- E. 3389
- F. SSH
- G. Terminal services
- H. Rlogin
- I. Rsync

J. Telnet

Answer: B,C,F,J

Explanation:

The question states that Jane was able to establish a connection to an internal router. Typical ports and protocols used to connect to a router include the following:

B, F: Port 22 which is used by SSH (Secure Shell).

C, J: Port 23 which is used by Telnet.

SSH and Telnet both provide command line interfaces for administering network devices such as routers and switches.

QUESTION NO: 672

Mike, a security professional, is tasked with actively verifying the strength of the security controls on a company's live modem pool. Which of the following activities is MOST appropriate?

- A. War dialing**
- B. War chalking**
- C. War driving**
- D. Bluesnarfing**

Answer: A

Explanation:

War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers - malicious hackers who specialize in computer security - for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.

QUESTION NO: 673

Which of the following is BEST utilized to actively test security controls on a particular system?

- A. Port scanning**
- B. Penetration test**
- C. Vulnerability scanning**
- D. Grey/Gray box**

Answer: B

Explanation:

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system.

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only

one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

QUESTION NO: 674

A security administrator is aware that a portion of the company's Internet-facing network tends to be non-secure due to poorly configured and patched systems. The business owner has accepted the risk of those systems being compromised, but the administrator wants to determine the degree to which those systems can be used to gain access to the company intranet. Which of the following should the administrator perform?

- A. Patch management assessment
- B. Business impact assessment
- C. Penetration test
- D. Vulnerability assessment

Answer: C

Explanation:

Penetration testing is the most intrusive type of testing because you are actively trying to circumvent the system's security controls to gain access to the system. It is also used to determine the degree to which the systems can be used to gain access to the company intranet (the degree of access to local network resources).

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

Targeted testing

Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see the test being carried out.

External testing

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

Internal testing

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

Blind testing

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

Double blind testing

Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.

QUESTION NO: 675

Ann, a security analyst, is preparing for an upcoming security audit. To ensure that she identifies unapplied security controls and patches without attacking or compromising the system, Ann would use which of the following?

- A. Vulnerability scanning
- B. SQL injection
- C. Penetration testing
- D. Antivirus update

Answer: A

Explanation:

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 676

Which of the following BEST represents the goal of a vulnerability assessment?

- A. To test how a system reacts to known threats
- B. To reduce the likelihood of exploitation
- C. To determine the system's security posture
- D. To analyze risk mitigation strategies

Answer: C

Explanation:

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 677

A security administrator wants to perform routine tests on the network during working hours when certain applications are being accessed by the most people. Which of the following would allow

the security administrator to test the lack of security controls for those applications with the least impact to the system?

- A. Penetration test
- B. Vulnerability scan
- C. Load testing
- D. Port scanner

Answer: B

Explanation:

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 678

Jane has recently implemented a new network design at her organization and wishes to passively identify security issues with the new network. Which of the following should Jane perform?

- A. Vulnerability assessment
- B. Black box testing
- C. White box testing
- D. Penetration testing

Answer: A

Explanation:

Vulnerability scanning has minimal impact on network resources due to the passive nature of the scanning.

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known

weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 679

A company hires outside security experts to evaluate the security status of the corporate network. All of the company's IT resources are outdated and prone to crashing. The company requests that all testing be performed in a way which minimizes the risk of system failures. Which of the following types of testing does the company want performed?

- A. Penetration testing
- B. WAF testing
- C. Vulnerability scanning
- D. White box testing

Answer: C

Explanation:

Vulnerability scanning has minimal impact on network resource due to the passive nature of the scanning.

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 680

Which of the following tests a number of security controls in the least invasive manner?

- A. Vulnerability scan
- B. Threat assessment
- C. Penetration test
- D. Ping sweep

Answer: A

Explanation:

Vulnerability scanning has minimal impact on network resource due to the passive nature of the scanning.

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 681

A company is looking to improve their security posture by addressing risks uncovered by a recent penetration test. Which of the following risks is MOST likely to affect the business on a day-to-day basis?

- A. Insufficient encryption methods
- B. Large scale natural disasters
- C. Corporate espionage
- D. Lack of antivirus software

Answer: D

Explanation:

The most common threat to computers is computer viruses. A computer can become infected with a virus through day-to-day activities such as browsing web sites or emails. As browsing and opening emails are the most common activities performed by all users, computer viruses represent the most likely risk to a business.

QUESTION NO: 682

Which of the following is BEST utilized to identify common misconfigurations throughout the enterprise?

- A. Vulnerability scanning
- B. Port scanning
- C. Penetration testing
- D. Black box

Answer: A

Explanation:

A vulnerability scan is the process of scanning the network and/or I.T. infrastructure for threats and vulnerabilities. The threats and vulnerabilities are then evaluated in a risk assessment and the necessary actions taken to resolve and vulnerabilities. A vulnerability scan scans for known weaknesses such as missing patches or security updates.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

QUESTION NO: 683

Which of the following is an example of a false positive?

- A. Anti-virus identifies a benign application as malware.
- B. A biometric iris scanner rejects an authorized user wearing a new contact lens.

- C. A user account is locked out after the user mistypes the password too many times.
- D. The IDS does not identify a buffer overflow.

Answer: A

Explanation:

A false positive is an error in some evaluation process in which a condition tested for is mistakenly found to have been detected.

In spam filters, for example, a false positive is a legitimate message mistakenly marked as UBE -- unsolicited bulk email, as junk email is more formally known. Messages that are determined to be spam -- whether correctly or incorrectly -- may be rejected by a server or client-side spam filter and returned to the sender as bounce e-mail.

One problem with many spam filtering tools is that if they are configured stringently enough to be effective, there is a fairly high chance of getting false positives. The risk of accidentally blocking an important message has been enough to deter many companies from implementing any anti-spam measures at all.

False positives are also common in security systems. A host intrusion prevention system (HIPS), for example, looks for anomalies, such as deviations in bandwidth, protocols and ports. When activity varies outside of an acceptable range -- for example, a remote application attempting to open a normally closed port -- an intrusion may be in progress. However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high.

False positives contrast with false negatives, which are results indicating mistakenly that some condition tested for is absent.

QUESTION NO: 684

Joe a company's new security specialist is assigned a role to conduct monthly vulnerability scans across the network. He notices that the scanner is returning a large amount of false positives or failed audits. Which of the following should Joe recommend to remediate these issues?

- A. Ensure the vulnerability scanner is located in a segmented VLAN that has access to the company's servers
- B. Ensure the vulnerability scanner is configured to authenticate with a privileged account
- C. Ensure the vulnerability scanner is attempting to exploit the weaknesses it discovers
- D. Ensure the vulnerability scanner is conducting antivirus scanning

Answer: A

Explanation:

The vulnerability scanner is returning false positives because it is trying to scan servers that it doesn't have access to; for example, servers on the Internet.

We need to ensure that the local network servers only are scanned. We can do this by locating the

vulnerability scanner in a segmented VLAN that has access to the company's servers.

A false positive is an error in some evaluation process in which a condition tested for is mistakenly found to have been detected.

In spam filters, for example, a false positive is a legitimate message mistakenly marked as UBE -- unsolicited bulk email, as junk email is more formally known. Messages that are determined to be spam -- whether correctly or incorrectly -- may be rejected by a server or client-side spam filter and returned to the sender as bounce e-mail.

One problem with many spam filtering tools is that if they are configured stringently enough to be effective, there is a fairly high chance of getting false positives. The risk of accidentally blocking an important message has been enough to deter many companies from implementing any anti-spam measures at all.

False positives are also common in security systems. A host intrusion prevention system (HIPS), for example, looks for anomalies, such as deviations in bandwidth, protocols and ports. When activity varies outside of an acceptable range -- for example, a remote application attempting to open a normally closed port -- an intrusion may be in progress. However, an anomaly, such as a sudden spike in bandwidth use, does not guarantee an actual attack, so this approach amounts to an educated guess and the chance for false positives can be high.

False positives contrast with false negatives, which are results indicating mistakenly that some condition tested for is absent.

QUESTION NO: 685

The Quality Assurance team is testing a new third party developed application. The Quality team does not have any experience with the application. Which of the following is the team performing?

- A.** Grey box testing
- B.** Black box testing
- C.** Penetration testing
- D.** White box testing

Answer: B

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain,

invariable output but is not aware of how the software produces the output in the first place.

QUESTION NO: 686

A process in which the functionality of an application is tested without any knowledge of the internal mechanisms of the application is known as:

- A. Black box testing
- B. White box testing
- C. Black hat testing
- D. Gray box testing

Answer: A

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well.

Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

QUESTION NO: 687

The security consultant is assigned to test a client's new software for security, after logs show targeted attacks from the Internet. To determine the weaknesses, the consultant has no access to the application program interfaces, code, or data structures. This is an example of which of the following types of testing?

- A. Black box
- B. Penetration
- C. Gray box
- D. White box

Answer: A

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to

virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well. Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

QUESTION NO: 688

Matt, the Chief Information Security Officer (CISO), tells the network administrator that a security company has been hired to perform a penetration test against his network. The security company asks Matt which type of testing would be most beneficial for him. Which of the following BEST describes what the security company might do during a black box test?

- A.** The security company is provided with all network ranges, security devices in place, and logical maps of the network.
- B.** The security company is provided with no information about the corporate network or physical locations.
- C.** The security company is provided with limited information on the network, including all network diagrams.
- D.** The security company is provided with limited information on the network, including some subnet ranges and logical network diagrams.

Answer: B

Explanation:

The term black box testing is generally associated with application testing. However, in this question the term is used for network testing. Black box testing means testing something when you have no knowledge of the inner workings.

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied to virtually every level of software testing: unit, integration, system and acceptance. It typically comprises most if not all higher level testing, but can also dominate unit testing as well. Specific knowledge of the application's code/internal structure and programming knowledge in general is not required. The tester is aware of what the software is supposed to do but is not aware of how it does it. For instance, the tester is aware that a particular input returns a certain, invariable output but is not aware of how the software produces the output in the first place.

QUESTION NO: 689

A quality assurance analyst is reviewing a new software product for security, and has complete access to the code and data structures used by the developers. This is an example of which of the following types of testing?

- A. Black box
- B. Penetration
- C. Gray box
- D. White box

Answer: D

Explanation:

White box testing is the process of testing an application when you have detailed knowledge of the inner workings of the application.

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases. The tester chooses inputs to exercise paths through the code and determine the appropriate outputs. This is analogous to testing nodes in a circuit, e.g. in-circuit testing (ICT).

White-box testing can be applied at the unit, integration and system levels of the software testing process. Although traditional testers tended to think of white-box testing as being done at the unit level, it is used for integration and system testing more frequently today. It can test paths within a unit, paths between units during integration, and between subsystems during a system-level test.

QUESTION NO: 690

Pete, a developer, writes an application. Jane, the security analyst, knows some things about the overall application but does not have all the details. Jane needs to review the software before it is released to production. Which of the following reviews should Jane conduct?

- A. Gray Box Testing
- B. Black Box Testing
- C. Business Impact Analysis
- D. White Box Testing

Answer: A

Explanation:

Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood.

Gray box testing can be contrasted with black box testing, a scenario in which the tester has no

knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests.

Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts.

QUESTION NO: 691

An IT auditor tests an application as an authenticated user. This is an example of which of the following types of testing?

- A.** Penetration
- B.** White box
- C.** Black box
- D.** Gray box

Answer: D

Explanation:

In this question, the tester is testing the application as an authenticated user. We can assume from this that the tester has at least limited knowledge of the application. This meets the criteria of a grey-box test.

Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood.

Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests.

Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts.

QUESTION NO: 692

A software development company has hired a programmer to develop a plug-in module to an existing proprietary application. After completing the module, the developer needs to test the entire application to ensure that the module did not introduce new vulnerabilities. Which of the following is the developer performing when testing the application?

- A. Black box testing
- B. White box testing
- C. Gray box testing
- D. Design review

Answer: C

Explanation:

In this question, we know the tester has some knowledge of the application because the tester developed a plug-in module for it. However, the tester does not have detailed information about the entire application. Therefore, this is a grey-box test.

Gray box testing, also called gray box analysis, is a strategy for software debugging in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood.

Gray box testing can be contrasted with black box testing, a scenario in which the tester has no knowledge or access to the internal workings of a program, or white box testing, a scenario in which the internal particulars are fully known. Gray box testing is commonly used in penetration tests.

Gray box testing is considered to be non-intrusive and unbiased because it does not require that the tester have access to the source code. With respect to internal processes, gray box testing treats a program as a black box that must be analyzed from the outside. During a gray box test, the person may know how the system components interact but not have detailed knowledge about internal program functions and operation. A clear distinction exists between the developer and the tester, thereby minimizing the risk of personnel conflicts.

QUESTION NO: 693

A set of standardized system images with a pre-defined set of applications is used to build end-user workstations. The security administrator has scanned every workstation to create a current inventory of all applications that are installed on active workstations and is documenting which applications are out-of-date and could be exploited. The security administrator is determining the:

- A. attack surface.
- B. application hardening effectiveness.
- C. application baseline.

D. OS hardening effectiveness.

Answer: A

Explanation:

In this question, we have out-of-date applications that could be exploited. The out-of-date applications are security vulnerabilities. The combination of all vulnerabilities that could be exploited (or attacked) is known as the attack surface.

The attack surface of a software environment is the sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment.

The basic strategies of attack surface reduction are to reduce the amount of code running, reduce entry points available to untrusted users, and eliminate services requested by relatively few users. One approach to improving information security is to reduce the attack surface of a system or software. By turning off unnecessary functionality, there are fewer security risks. By having less code available to unauthorized actors, there will tend to be fewer failures. Although attack surface reduction helps prevent security failures, it does not mitigate the amount of damage an attacker could inflict once a vulnerability is found.

QUESTION NO: 694

On a train, an individual is watching a proprietary video on Joe's laptop without his knowledge. Which of the following does this describe?

- A. Tailgating
- B. Shoulder surfing
- C. Interference
- D. Illegal downloading

Answer: B

Explanation:

Looking at information on a computer screen without the computer user's knowledge is known as shoulder surfing.

Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done long distance with the aid of binoculars or other vision-enhancing devices. To prevent shoulder surfing, experts recommend that you shield paperwork or your keypad from view by using your body or cupping your hand.

QUESTION NO: 695

Which of the following devices is used for the transparent security inspection of network traffic by redirecting user packets prior to sending the packets to the intended destination?

- A. Proxies
- B. Load balancers
- C. Protocol analyzer
- D. VPN concentrator

Answer: A

Explanation:

A proxy is a device that acts on behalf of other(s). A commonly used proxy in computer networks is a web proxy. Web proxy functionality is often combined into a proxy firewall.

A proxy firewall can be thought of as an intermediary between your network and any other network. Proxy firewalls are used to process requests from an outside network; the proxy firewall examines the data and makes rule-based decisions about whether the request should be forwarded or refused. The proxy intercepts all of the packets and reprocesses them for use internally. This process includes hiding IP addresses.

The proxy firewall provides better security than packet filtering because of the increased intelligence that a proxy firewall offers. Requests from internal network users are routed through the proxy. The proxy, in turn, repackages the request and sends it along, thereby isolating the user from the external network. The proxy can also offer caching, should the same request be made again, and it can increase the efficiency of data delivery.

QUESTION NO: 696

An administrator is investigating a system that may potentially be compromised, and sees the following log entries on the router.

*Jul 15 14:47:29.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 3 packets.

*Jul 15 14:47:38.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 6 packets.

*Jul 15 14:47:45.779:%Router1: list 101 permitted tcp 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 8 packets.

Which of the following BEST describes the compromised system?

- A. It is running a rogue web server
- B. It is being used in a man-in-the-middle attack
- C. It is participating in a botnet
- D. It is an ARP poisoning attack

Answer: C

Explanation:

In this question, we have a source computer (192.10.3.204) sending data to a single destination IP address 10.10.1.5. No data is being received back by source computer which suggests the data being sent is some kind of Denial-of-service attack. This is common practice for computers participating in a botnet. The port used is TCP 6667 which is IRC (Internet Relay Chat). This port is used by many Trojans and is commonly used for DoS attacks.

Software running on infected computers called zombies is often known as a botnet. Bots, by themselves, are but a form of software that runs automatically and autonomously. (For example, Google uses the Googlebot to find web pages and bring back values for the index.)

Botnet, however, has come to be the word used to describe malicious software running on a zombie and under the control of a bot-herder.

Denial-of-service attacks—DoS and DDoS—can be launched by botnets, as can many forms of malware, spyware, and spam (via spambots). Most bots are written to run in the background with no visible evidence of their presence. Many malware kits can be used to create botnets and modify existing ones.

QUESTION NO: 697

The Chief Executive Officer (CEO) receives a suspicious voice mail warning of credit card fraud. No one else received the voice mail. Which of the following BEST describes this attack?

- A. Whaling
- B. Vishing
- C. Spear phishing
- D. Impersonation

Answer: A

Explanation:

Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles.

Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data

theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.

QUESTION NO: 698

An administrator was asked to review user accounts. Which of the following has the potential to cause the MOST amount of damage if the account was compromised?

- A. A password that has not changed in 180 days
- B. A single account shared by multiple users
- C. A user account with administrative rights
- D. An account that has not been logged into since creation

Answer: C

Explanation:

A user account with administrative rights has the same rights as an administrator account on a computer.

An administrator account is a user account that lets you make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. Administrators can also make changes to other user accounts.

This compares to a standard user (non-administrative) account which has limited rights on a computer. For example, a standard user account cannot install software, cannot make system changes that would affect other users and cannot access other users' files.

Therefore, a compromised user account with administrative rights has the potential for the most damage.

QUESTION NO: 699

Failure to validate the size of a variable before writing it to memory could result in which of the following application attacks?

- A. Malicious logic
- B. Cross-site scripting
- C. SQL injection
- D. Buffer overflow

Answer: D

Explanation:

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information.

Validating the size of a variable before writing it to memory will ensure that the variable can fit into the buffer. Failure to validate the size of a variable before writing it to memory can result in a buffer overflow.

QUESTION NO: 700

During a disaster recovery planning session, a security administrator has been tasked with determining which threats and vulnerabilities pose a risk to the organization. Which of the following should the administrator rate as having the HIGHEST frequency of risk to the organization?

- A. Hostile takeovers
- B. Large scale natural disasters
- C. Malware and viruses
- D. Corporate espionage

Answer: C

Explanation:

The most common threat to an organization is computer viruses or malware. A computer can become infected with a virus through day-to-day activities such as browsing web sites or emails. As browsing and opening emails are the most common activities performed by all users, computer viruses represent the most likely risk to a business.

Common examples of malware include viruses, worms, trojan horses, and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it. This can include anything from the Web pages a user visits to personal information, such as credit card numbers.

QUESTION NO: 701

Company XYZ has encountered an increased amount of buffer overflow attacks. The programmer

has been tasked to identify the issue and report any findings. Which of the following is the FIRST step of action recommended in this scenario?

- A. Baseline Reporting
- B. Capability Maturity Model
- C. Code Review
- D. Quality Assurance and Testing

Answer: C

Explanation:

A buffer overflow attack attacks a vulnerability caused by poor coding in an application. Reviewing the code of the application will enable you to identify code that is vulnerable to buffer overflow.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user's files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

QUESTION NO: 702

Which of the following is a penetration testing method?

- A. Searching the WHOIS database for administrator contact information
- B. Running a port scanner against the target's network
- C. War driving from a target's parking lot to footprint the wireless network
- D. Calling the target's helpdesk, requesting a password reset

Answer: D

Explanation:

A penetration test is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-users' adherence to security policies.

Penetration testing evaluates an organization's ability to protect its networks, applications,

endpoints and users from external or internal attempts to circumvent its security controls to gain unauthorized or privileged access to protected assets. Test results validate the risk posed by specific security vulnerabilities or flawed processes, enabling IT management and security professionals to prioritize remediation efforts. By embracing more frequent and comprehensive penetration testing, organizations can more effectively anticipate emerging security risks and prevent unauthorized access to critical systems and valuable information.

Penetration tests are not always technically clever attempts to access a network. By calling the target's helpdesk and requesting a password reset, if they reset the password without requiring proof that you are authorized to request a password change, you can easily gain access to the network.

QUESTION NO: 703

Which of the following would MOST likely involve GPS?

- A. Wardriving
- B. Protocol analyzer
- C. Replay attack
- D. WPS attack

Answer: A

Explanation:

War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, you need a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car. A GPS (Global Positioning System) system can be used to accurately map your location while detecting the wireless networks.

QUESTION NO: 704

The system administrator is reviewing the following logs from the company web server:

12:34:56 GET /directory_listing.php?user=admin&pass=admin1

12:34:57 GET /directory_listing.php?user=admin&pass=admin2

12:34:58 GET /directory_listing.php?user=admin&pass=1admin

12:34:59 GET /directory_listing.php?user=admin&pass=2admin

Which of the following is this an example of?

- A. Online rainbow table attack
- B. Offline brute force attack
- C. Offline dictionary attack
- D. Online hybrid attack

Answer: D

Explanation:

This is an example of an online hybrid attack. A hybrid attack is a combination of attacks. In this example, we have a combination of a dictionary attack and a brute-force attack.

A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data.

A dictionary attack uses a list of words to use as passwords. The combination or hybrid attack adds characters or numbers or even other words to the beginning or end of the password guesses. In this example we have a password guess of 'admin'. From the word admin, we have four combinations, 'admin1, 1admin, admin2, 2admin'.

QUESTION NO: 705

A large multinational corporation with networks in 30 countries wants to establish an understanding of their overall public-facing network attack surface. Which of the following security techniques would be BEST suited for this?

- A. External penetration test
- B. Internal vulnerability scan
- C. External vulnerability scan
- D. Internal penetration test

Answer: C

Explanation:

In this question, we need to determine the public-facing network attack surface. We therefore need to perform a vulnerability scan from outside the network; in other words, an external vulnerability scan.

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.

Vulnerability scanning employs software that seeks out security flaws based on a database of

known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

QUESTION NO: 706

Which of the following attacks impact the availability of a system? (Select TWO).

- A. Smurf
- B. Phishing
- C. Spim
- D. DDoS
- E. Spoofing

Answer: A,D

Explanation:

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to its knees.

Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

A Distributed Denial of Service (DDoS) attack is an attack from several different computers targeting a single computer.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are

that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply add more attack machines. This after all will end up completely crashing a website for periods of time.

QUESTION NO: 707

Which of the following types of technologies is used by security and research personnel for identification and analysis of new security threats in a networked environment by using false data/hosts for information collection?

- A. Honeynet
- B. Vulnerability scanner
- C. Port scanner
- D. Protocol analyzer

Answer: A

Explanation:

A honeynet is a network set up with intentional vulnerabilities; its purpose is to invite attack, so that an attacker's activities and methods can be studied and that information used to increase network security. A honeynet contains one or more honey pots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. Although the primary purpose of a honeynet is to gather information about attackers' methods and motives, the decoy network can benefit its operator in other ways, for example by diverting attackers from a real network and its resources. The Honeynet Project, a non-profit research organization dedicated to computer security and information sharing, actively promotes the deployment of honeynets.

In addition to the honey pots, a honeynet usually has real applications and services so that it seems like a normal network and a worthwhile target. However, because the honeynet doesn't actually serve any authorized users, any attempt to contact the network from without is likely an illicit attempt to breach its security, and any outbound activity is likely evidence that a system has been compromised. For this reason, the suspect information is much more apparent than it would be in an actual network, where it would have to be found amidst all the legitimate network data. Applications within a honeynet are often given names such as "Finances" or "Human Services" to make them sound appealing to the attacker.

QUESTION NO: 708

A computer is found to be infected with malware and a technician re-installs the operating system. The computer remains infected with malware. This is an example of:

- A. a rootkit.
- B. a MBR infection.
- C. an exploit kit.
- D. Spyware.

Answer: B

Explanation:

An MBR infection is malware that is installed into the Master Boot Record (MBR) of a hard disk. Reinstalling the operating system does not remove the malware from the MBR. A 'Bootkit' is a rootkit that infects the Master Boot Record.

Bootkits are an advanced form of rootkits that take the basic functionality of a rootkit and extend it with the ability to infect the master boot record (MBR) or volume boot record (VBR) so that the bootkit remains active even after a system reboot.

Bootkits are designed to not only load from the master boot record but also remain active in the system memory from protected mode through the launch of the operating system and during the computer's active state.

QUESTION NO: 709

A user has plugged in a wireless router from home with default configurations into a network jack at the office. This is known as:

- A. an evil twin.
- B. an IV attack.
- C. a rogue access point.
- D. an unauthorized entry point.

Answer: C

Explanation:

A rogue access point is a wireless access point that should not be there. In this question, the wireless router has been connected to the corporate network without authorization. Therefore, it is a rogue access point.

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with

access to the premises can install (maliciously or non-maliciously) an inexpensive wireless router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in conjunction with a rogue RADIUS server, depending on security configuration of the target network.

To prevent the installation of rogue access points, organizations can install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points.

QUESTION NO: 710

Four weeks ago, a network administrator applied a new IDS and allowed it to gather baseline data. As rumors of a layoff began to spread, the IDS alerted the network administrator that access to sensitive client files had risen far above normal. Which of the following kind of IDS is in use?

- A.** Protocol based
- B.** Heuristic based
- C.** Signature based
- D.** Anomaly based

Answer: D

Explanation:

Most intrusion detection systems (IDS) are what is known as signature-based. This means that they operate in much the same way as a virus scanner, by searching for a known identity - or signature - for each specific intrusion event. And, while signature-based IDS is very efficient at sniffing out known methods of attack, it does, like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker technique. In other words, signature-based IDS is only as good as its database of stored signatures.

Any organization wanting to implement a more thorough - and hence safer - solution, should consider what we call anomaly-based IDS. By its nature, anomaly-based IDS is a rather more complex creature. In network traffic terms, it captures all the headers of the IP packets running towards the network. From this, it filters out all known and legal traffic, including web traffic to the organization's web server, mail traffic to and from its mail server, outgoing web traffic from company employees and DNS traffic to and from its DNS server.

There are other equally obvious advantages to using anomaly-based IDS. For example, because it detects any traffic that is new or unusual, the anomaly method is particularly good at identifying sweeps and probes towards network hardware. It can, therefore, give early warnings of potential intrusions, because probes and scans are the predecessors of all attacks. And this applies equally to any new service installed on any item of hardware - for example, Telnet deployed on a network router for maintenance purposes and forgotten about when the maintenance was finished. This

makes anomaly-based IDS perfect for detecting anything from port anomalies and web anomalies to mis-formed attacks, where the URL is deliberately mis-typed.

QUESTION NO: 711

A security administrator is notified that users attached to a particular switch are having intermittent connectivity issues. Upon further research, the administrator finds evidence of an ARP spoofing attack. Which of the following could be utilized to provide protection from this type of attack?

- A. Configure MAC filtering on the switch.
- B. Configure loop protection on the switch.
- C. Configure flood guards on the switch.
- D. Configure 802.1x authentication on the switch.

Answer: C

Explanation:

ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing can enable malicious parties to intercept, modify or even stop data in-transit. ARP spoofing attacks can only occur on local area networks that utilize the Address Resolution Protocol.

To perform ARP spoofing the attacker floods the network with spoofed ARP packets. As other hosts on the LAN cache the spoofed ARP packets, data that those hosts send to the victim will go to the attacker instead. From here, the attacker can steal data or launch a more sophisticated follow-up attack.

A flood guard configured on the network switch will block the flood of spoofed ARP packets.

QUESTION NO: 712

An organization must implement controls to protect the confidentiality of its most sensitive data. The company is currently using a central storage system and group based access control for its sensitive information. Which of the following controls can further secure the data in the central storage system?

- A. Data encryption
- B. Patching the system

- C. Digital signatures
- D. File hashing

Answer: A

Explanation:

Data encryption makes data unreadable to anyone who does not have the required key to decrypt the data. The question states that the sensitive data is stored on a central storage system. Group based access control is used to control who can access the sensitive data. However, this offers no physical security for the data. Someone could steal the central storage system or remove the hard disks from it with the plan of placing the hard disks into another system to read the data on the disks. With the data encrypted, the data would be unreadable.

QUESTION NO: 713

Joe, the information security manager, is tasked with calculating risk and selecting controls to protect a new system. He has identified people, environmental conditions, and events that could affect the new system. Which of the following does he need to estimate NEXT in order to complete his risk calculations?

- A. Vulnerabilities
- B. Risk
- C. Likelihood
- D. Threats

Answer: A

Explanation:

In this question, the security administrator has identified people, environmental conditions, and events that could affect the new system. The next step of the risk assessment is to determine the vulnerabilities of the system itself.

Risk assessment deals with the threats, vulnerabilities, and impacts of a loss of information-processing capabilities or a loss of information itself. A vulnerability is a weakness that could be exploited by a threat. Each risk that can be identified should be outlined, described, and evaluated for the likelihood of it occurring. The key here is to think outside the box. Conventional threats and risks are often too limited when considering risk assessment.

The key components of a risk-assessment process are outlined here:

Risks to Which the Organization Is Exposed: This component allows you to develop scenarios that can help you evaluate how to deal with these risks if they occur. An operating system, server, or application may have known risks in certain environments. You should create a plan for how your organization will best deal with these risks and the best way to respond.

Risks That Need Addressing: The risk-assessment component also allows an organization to

provide a reality check on which risks are real and which are unlikely. This process helps an organization focus on its resources as well as on the risks that are most likely to occur. For example, industrial espionage and theft are likely, but the risk of a hurricane damaging the server room in Indiana is very low. Therefore, more resources should be allocated to prevent espionage or theft as opposed to the latter possibility.

QUESTION NO: 714

A network administrator identifies sensitive files being transferred from a workstation in the LAN to an unauthorized outside IP address in a foreign country. An investigation determines that the firewall has not been altered, and antivirus is up-to-date on the workstation. Which of the following is the MOST likely reason for the incident?

- A. MAC Spoofing
- B. Session Hijacking
- C. Impersonation
- D. Zero-day

Answer: D

Explanation:

This question states that antivirus is up-to-date on the workstation and the firewall has not been altered. The antivirus software is up to date with all 'known' viruses. A zero day vulnerability is an unknown vulnerability so a patch or virus definition has not been released yet.

A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term "zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

QUESTION NO: 715

A security administrator must implement a network that is immune to ARP spoofing attacks. Which of the following should be implemented to ensure that a malicious insider will not be able to successfully use ARP spoofing techniques?

- A. UDP
- B. IPv6

- C. IPSec
- D. VPN

Answer: B

Explanation: ARP is not used in IPv6 networks.

The Address Resolution Protocol (ARP) is a telecommunication protocol used for resolution of network layer addresses into link layer addresses, a critical function in multiple-access networks. ARP is used for converting a network address (e.g. an IPv4 address) to a physical address like an Ethernet address (also named a MAC address).

In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).

QUESTION NO: 716

After working on his doctoral dissertation for two years, Joe, a user, is unable to open his dissertation file. The screen shows a warning that the dissertation file is corrupted because it is infected with a backdoor, and can only be recovered by upgrading the antivirus software from the free version to the commercial version. Which of the following types of malware is the laptop MOST likely infected with?

- A. Ransomware
- B. Trojan
- C. Backdoor
- D. Armored virus

Answer: A

Explanation:

Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive), while some may simply lock the system and display messages intended to coax the user into paying.

Ransomware typically propagates as a trojan like a conventional computer worm, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program will then run a payload: such as one that will begin to encrypt personal files on the hard drive. More sophisticated ransomware may hybrid-encrypt the victim's plaintext with a random symmetric key and a fixed public key. The malware author is the only party that knows the needed private decryption key. Some ransomware payloads do not use encryption. In these cases, the payload is simply an application designed to restrict interaction with the system, typically by setting the Windows Shell to itself, or even modifying the master boot record and/or partition table (which prevents the operating system from booting at all until it is repaired)

Ransomware payloads utilize elements of scareware to extort money from the system's user. The payload may, for example, display notices purportedly issued by companies or law enforcement agencies which falsely claim that the system had been used for illegal activities, or contains illegal content such as pornography and pirated software or media. Some ransomware payloads imitate Windows' product activation notices, falsely claiming that their computer's Windows installation is counterfeit or requires re-activation. These tactics coax the user into paying the malware's author to remove the ransomware, either by supplying a program which can decrypt the files, or by sending an unlock code that undoes the changes the payload has made.

QUESTION NO: 717

An employee connects a wireless access point to the only jack in the conference room to provide Internet access during a meeting. The access point is configured to use WPA2-TKIP. A malicious user is able to intercept clear text HTTP communication between the meeting attendees and the Internet. Which of the following is the reason the malicious user is able to intercept and see the clear text communication?

- A. The malicious user has access to the WPA2-TKIP key.
- B. The wireless access point is broadcasting the SSID.
- C. The malicious user is able to capture the wired communication.
- D. The meeting attendees are using unencrypted hard drives.

Answer: C

Explanation:

In this question, the wireless users are using WPA2-TKIP. While TKIP is a weak encryption protocol, it is still an encryption protocol. Therefore, the wireless communications between the laptops and the wireless access point are encrypted.

The question states that user was able to intercept 'clear text' HTTP communication between the meeting attendees and the Internet. The HTTP communications are unencrypted as they travel over the wired network. Therefore, the malicious user must have been able to capture the wired communication.

TKIP and AES are two different types of encryption that can be used by a Wi-Fi network. TKIP stands for "Temporal Key Integrity Protocol." It was a stopgap encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time. TKIP is actually quite similar to WEP encryption. TKIP is no longer considered secure, and is now deprecated.

QUESTION NO: 718

Which of the following password attacks is MOST likely to crack the largest number of randomly

generated passwords?

- A. Hybrid
- B. Birthday attack
- C. Dictionary
- D. Rainbow tables

Answer: D

Explanation:

When a password is "tried" against a system it is "hashed" using encryption so that the actual password is never sent in clear text across the communications line. This prevents eavesdroppers from intercepting the password. The hash of a password usually looks like a bunch of garbage and is typically a different length than the original password. Your password might be "shitzu" but the hash of your password would look something like "7378347eedbfdd761619451949225ec1".

To verify a user, a system takes the hash value created by the password hashing function on the client computer and compares it to the hash value stored in a table on the server. If the hashes match, then the user is authenticated and granted access.

Password cracking programs work in a similar way to the login process. The cracking program starts by taking plaintext passwords, running them through a hash algorithm, such as MD5, and then compares the hash output with the hashes in the stolen password file. If it finds a match then the program has cracked the password.

Rainbow Tables are basically huge sets of precomputed tables filled with hash values that are pre-matched to possible plaintext passwords. The Rainbow Tables essentially allow hackers to reverse the hashing function to determine what the plaintext password might be.

The use of Rainbow Tables allow for passwords to be cracked in a very short amount of time compared with brute-force methods, however, the trade-off is that it takes a lot of storage (sometimes Terabytes) to hold the Rainbow Tables themselves.

With a rainbow table, all of the possible hashes are computed in advance. In other words, you create a series of tables; each has all the possible two-letter, three-letter, four-letter, and so forth combinations and the hash of that combination, using a known hashing algorithm like SHA-2. Now if you search the table for a given hash, the letter combination in the table that produced the hash must be the password you are seeking.

QUESTION NO: 719

Which of the following attacks involves the use of previously captured network traffic?

- A. Replay
- B. Smurf

- C. Vishing
- D. DDoS

Answer: A

Explanation:

Replay attacks are becoming quite common. They occur when information is captured over a network. A replay attack is a kind of access or modification attack. In a distributed environment, logon and password information is sent between the client and the authentication system. The attacker can capture the information and replay it later. This can also occur with security certificates from systems such as Kerberos: The attacker resubmits the certificate, hoping to be validated by the authentication system and circumvent any time sensitivity.

If this attack is successful, the attacker will have all of the rights and privileges from the original certificate. This is the primary reason that most certificates contain a unique session identifier and a time stamp. If the certificate has expired, it will be rejected and an entry should be made in a security log to notify system administrators.

QUESTION NO: 720

An attacker crafts a message that appears to be from a trusted source, but in reality it redirects the recipient to a malicious site where information is harvested. The message is narrowly tailored so it is effective on only a small number of victims. This describes which of the following?

- A. Spear phishing
- B. Phishing
- C. Smurf attack
- D. Vishing

Answer: A

Explanation:

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

QUESTION NO: 721

An administrator is instructed to disable IP-directed broadcasts on all routers in an organization. Which of the following attacks does this prevent?

- A. Pharming
- B. Smurf
- C. Replay
- D. Xmas

Answer: B

Explanation:

A smurf attack is a type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's Internet connection with ping replies, bringing their entire Internet service to its knees. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

By disabling IP-directed broadcasts on all routers, we can prevent the smurf attack by blocking the ping requests to broadcast addresses.

QUESTION NO: 722

An administrator has to determine host operating systems on the network and has deployed a transparent proxy. Which of the following fingerprint types would this solution use?

- A. Packet
- B. Active
- C. Port
- D. Passive

Answer: D

Explanation:

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote machine's operating system (aka, OS fingerprinting), or incorporated into a device fingerprint.

Certain parameters within the TCP protocol definition are left up to the implementation. Different operating systems and different versions of the same operating system set different defaults for these values. By collecting and examining these values, one may differentiate among various operating systems, and implementations of TCP/IP. Just inspecting the Initial TTL and window size TCP/IP fields is often enough in order to successfully identify an operating system, which eases the task of performing manual OS fingerprinting.

Passive OS fingerprinting is the examination of a passively collected sample of packets from a host in order to determine its operating system platform. It is called passive because it doesn't involve communicating with the host being examined.

In this question, the proxy will use passive fingerprinting because the proxy is a 'transparent proxy'. It isn't seen by the computer.

QUESTION NO: 723

An internal audit has detected that a number of archived tapes are missing from secured storage. There was no recent need for restoration of data from the missing tapes. The location is monitored by access control and CCTV systems. Review of the CCTV system indicates that it has not been recording for three months. The access control system shows numerous valid entries into the storage location during that time. The last audit was six months ago and the tapes were accounted for at that time. Which of the following could have aided the investigation?

- A.** Testing controls
- B.** Risk assessment
- C.** Signed AUP
- D.** Routine audits

Answer: A

Explanation:

Testing controls come in three types: Technical, Management and Operational.

In this question, the CCTV system has not been recording for three months and no one noticed. Improved testing controls (regular testing to verify the CCTV system is recording) would ensure that the CCTV is recording as expected.

The CCTV recordings could have aided the investigation into the missing tapes.

Topic 4, Application, Data and Host Security

QUESTION NO: 724

Methods to test the responses of software and web applications to unusual or unexpected inputs are known as:

- A. Brute force.
- B. HTML encoding.
- C. Web crawling.
- D. Fuzzing.

Answer: D

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 725

Which of the following application security testing techniques is implemented when an automated system generates random input data?

- A. Fuzzing
- B. XSRF
- C. Hardening
- D. Input validation

Answer: A

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 726

Which of the following security concepts identifies input variables which are then used to perform boundary testing?

- A. Application baseline
- B. Application hardening
- C. Secure coding
- D. Fuzzing

Answer: D

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 727

Which of the following describes purposefully injecting extra input during testing, possibly causing an application to crash?

- A. Input validation
- B. Exception handling
- C. Application hardening
- D. Fuzzing

Answer: D

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 728

A security administrator wants to test the reliability of an application which accepts user provided parameters. The administrator is concerned with data integrity and availability. Which of the following should be implemented to accomplish this task?

- A. Secure coding
- B. Fuzzing
- C. Exception handling
- D. Input validation

Answer: B

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 729

Fuzzing is a security assessment technique that allows testers to analyze the behavior of software applications under which of the following conditions?

- A. Unexpected input
- B. Invalid output
- C. Parameterized input
- D. Valid output

Answer: A

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 730

Which of the following application security principles involves inputting random data into a program?

- A. Brute force attack
- B. Sniffing
- C. Fuzzing
- D. Buffer overflow

Answer: C

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 731

An IT security technician is actively involved in identifying coding issues for her company.

Which of the following is an application security technique that can be used to identify unknown

weaknesses within the code?

- A. Vulnerability scanning
- B. Denial of service
- C. Fuzzing
- D. Port scanning

Answer: C

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 732

Which of the following would Jane, an administrator, use to detect an unknown security vulnerability?

- A. Patch management
- B. Application fuzzing
- C. ID badge
- D. Application configuration baseline

Answer: B

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 733

Which of the following pseudocodes can be used to handle program exceptions?

- A. If program detects another instance of itself, then kill program instance.
- B. If user enters invalid input, then restart program.
- C. If program module crashes, then restart program module.
- D. If user's input exceeds buffer length, then truncate the input.

Answer: C

Explanation:

Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture all errors and exceptions that could cause the application or its modules to crash. Restarting the application or module would ensure that the application reverts back to a secure state.

QUESTION NO: 734

Which of the following is an application security coding problem?

- A. Error and exception handling
- B. Patch management
- C. Application hardening
- D. Application fuzzing

Answer: A

Explanation:

Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application.

QUESTION NO: 735

Sara, an application developer, implemented error and exception handling alongside input validation. Which of the following does this help prevent?

- A. Buffer overflow
- B. Pop-up blockers
- C. Cross-site scripting
- D. Fuzzing

Answer: A

Explanation:

Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

QUESTION NO: 736

Which of the following techniques can be used to prevent the disclosure of system information resulting from arbitrary inputs when implemented properly?

- A. Fuzzing
- B. Patch management
- C. Error handling
- D. Strong passwords

Answer: C

Explanation:

Exception handling is an aspect of secure coding. When errors occur, the system should revert back to a secure state. This must be coded into the system by the programmer, and should capture errors and exceptions so that they could be handled by the application.

QUESTION NO: 737

A program displays:

ERROR: this program has caught an exception and will now terminate.

Which of the following is MOST likely accomplished by the program's behavior?

- A. Operating system's integrity is maintained
- B. Program's availability is maintained
- C. Operating system's scalability is maintained
- D. User's confidentiality is maintained

Answer: A

Explanation:

The purpose of error handling is to maintain the security and integrity of the system. Integrity is compromised when unauthorized modification occurs.

QUESTION NO: 738

Which of the following is a best practice for error and exception handling?

- A. Log detailed exception but display generic error message
- B. Display detailed exception but log generic error message
- C. Log and display detailed error and exception messages
- D. Do not log or display error or exception messages

Answer: A

Explanation:

A detailed explanation of the error is not helpful for most end users but might provide information that is useful to a hacker. It is therefore better to display a simple but helpful message to the end user and log the detailed information to an access-restricted log file for the administrator and programmer who would need as much information as possible about the problem in order to rectify it.

QUESTION NO: 739

Which of the following is true about input validation in a client-server architecture, when data integrity is critical to the organization?

- A. It should be enforced on the client side only.
- B. It must be protected by SSL encryption.
- C. It must rely on the user's knowledge of the application.
- D. It should be performed on the server side.

Answer: D

Explanation:

Client-side validation should only be used to improve user experience, never for security purposes. A client-side input validation check can improve application performance by catching malformed input on the client and, therefore, saving a roundtrip to the server. However, client side validation can be easily bypassed and should never be used for security purposes. Always use server-side validation to protect your application from malicious attacks.

QUESTION NO: 740

Which of the following is the below pseudo-code an example of?

IF VARIABLE (CONTAINS NUMBERS = TRUE) THEN EXIT

- A. Buffer overflow prevention
- B. Input validation

- C. CSRF prevention
- D. Cross-site scripting prevention

Answer: B

Explanation:

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

QUESTION NO: 741

After Matt, a user, enters his username and password at the login screen of a web enabled portal, the following appears on his screen:

`Please only use letters and numbers on these fields'

Which of the following is this an example of?

- A. Proper error handling
- B. Proper input validation
- C. Improper input validation
- D. Improper error handling

Answer: B

Explanation:

Input validation is an aspect of secure coding and is intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

QUESTION NO: 742

In regards to secure coding practices, why is input validation important?

- A. It mitigates buffer overflow attacks.
- B. It makes the code more readable.
- C. It provides an application configuration baseline.
- D. It meets gray box testing standards.

Answer: A

Explanation:

Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

QUESTION NO: 743

Input validation is an important security defense because it:

- A. rejects bad or malformed data.
- B. enables verbose error reporting.
- C. protects mis-configured web servers.
- D. prevents denial of service attacks.

Answer: A

Explanation:

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

QUESTION NO: 744

Which of the following is a common coding error in which boundary checking is not performed?

- A. Input validation
- B. Fuzzing
- C. Secure coding
- D. Cross-site scripting

Answer: A

Explanation:

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a

language type, or a domain.

QUESTION NO: 745

One of the most consistently reported software security vulnerabilities that leads to major exploits is:

- A. Lack of malware detection.
- B. Attack surface decrease.
- C. Inadequate network hardening.
- D. Poor input validation.

Answer: D

Explanation:

D: With coding there are standards that should be observed. Of these standards the most fundamental is input validation. Attacks such as SQL injection depend on unfiltered input being sent through a web application. This makes for a software vulnerability that can be exploited. There are two primary ways to do input validation: client-side validation and server-side validation. Thus with poor input validation you increase your risk with regard to exposure to major software exploits.

QUESTION NO: 746

Without validating user input, an application becomes vulnerable to all of the following EXCEPT:

- A. Buffer overflow.
- B. Command injection.
- C. Spear phishing.
- D. SQL injection.

Answer: C

Explanation:

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

QUESTION NO: 747

Which of the following can BEST help prevent cross-site scripting attacks and buffer overflows on a production system?

- A. Input validation
- B. Network intrusion detection system
- C. Anomaly-based HIDS
- D. Peer review

Answer: A

Explanation:

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

QUESTION NO: 748

The BEST methods for a web developer to prevent the website application code from being vulnerable to cross-site request forgery (XSRF) are to: (Select TWO).

- A. Permit redirection to Internet-facing web URLs.
- B. Ensure all HTML tags are enclosed in angle brackets, e.g., "<" and ">".
- C. Validate and filter input on the server side and client side.
- D. Use a web proxy to pass website requests between the user and the application.
- E. Restrict and sanitize use of special characters in input and URLs.

Answer: C,E

Explanation:

XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is often accomplished without the user's knowledge.

XSRF can be prevented by adding a randomization string (called a nonce) to each URL request and session establishment and checking the client HTTP request header referrer for spoofing.

QUESTION NO: 749

After visiting a website, a user receives an email thanking them for a purchase which they did not request. Upon investigation the security administrator sees the following source code in a pop-up

window:

```
<HTML>
```

```
<body onload="document.getElementById('badForm').submit()">
```

```
<form id="badForm" action="shoppingsite.company.com/purchase.php" method="post" >
```

```
<input name="Perform Purchase" value="Perform Purchase"/>
```

```
</form>
```

```
</body>
```

```
</HTML>
```

Which of the following has MOST likely occurred?

- A. SQL injection
- B. Cookie stealing
- C. XSRF
- D. XSS

Answer: C

Explanation:

XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is often accomplished without the user's knowledge.

QUESTION NO: 750

Which of the following is the BEST way to prevent Cross-Site Request Forgery (XSRF) attacks?

- A. Check the referrer field in the HTTP header
- B. Disable Flash content
- C. Use only cookies for authentication
- D. Use only HTTPS URLs

Answer: A

Explanation:

XSRF or cross-site request forgery applies to web applications and is an attack that exploits the web application's trust of a user who known or is supposed to have been authenticated. This is accomplished by changing values in the HTTP header and even in the user's cookie to falsify

access. It can be prevented by embedding additional authentication data into requests that allows the web application to detect requests from unauthorized locations. Examples are synchronizer token patterns, cookie-to-header tokens, and checking the HTTP Referrer header and the HTTP Origin header.

QUESTION NO: 751

The process of making certain that an entity (operating system, application, etc.) is as secure as it can be is known as:

- A. Stabilizing
- B. Reinforcing
- C. Hardening
- D. Toughening

Answer: C

Explanation:

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

QUESTION NO: 752

Vendors typically ship software applications with security settings disabled by default to ensure a wide range of interoperability with other applications and devices. A security administrator should perform which of the following before deploying new software?

- A. Application white listing
- B. Network penetration testing
- C. Application hardening
- D. Input fuzzing testing

Answer: C

Explanation:

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

QUESTION NO: 753

Which of the following describes the process of removing unnecessary accounts and services from an application to reduce risk exposure?

- A. Error and exception handling
- B. Application hardening
- C. Application patch management
- D. Cross-site script prevention

Answer: B

Explanation:

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

QUESTION NO: 754

A network administrator is responsible for securing applications against external attacks. Every month, the underlying operating system is updated. There is no process in place for other software updates.

Which of the following processes could MOST effectively mitigate these risks?

- A. Application hardening
- B. Application change management
- C. Application patch management
- D. Application firewall review

Answer: C

Explanation:

The question states that operating system updates are applied but not other software updates. The 'other software' in this case would be applications. Software updates includes functionality updates and more importantly security updates. The process of applying software updates or 'patches' to applications is known as 'application patch management'. Application patch management is an effective way of mitigating security risks associated with software applications.

QUESTION NO: 755

A recently installed application update caused a vital application to crash during the middle of the

workday. The application remained down until a previous version could be reinstalled on the server, and this resulted in a significant loss of data and revenue.

Which of the following could BEST prevent this issue from occurring again?

- A. Application configuration baselines
- B. Application hardening
- C. Application access controls
- D. Application patch management

Answer: D

Explanation:

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system first to ensure that the updates do not have detrimental effects on the system, and, should the updates have no detrimental effects on the test systems, backing up the production systems before applying the updates on a production system.

QUESTION NO: 756

An administrator finds that non-production servers are being frequently compromised, production servers are rebooting at unplanned times and kernel versions are several releases behind the version with all current security fixes.

Which of the following should the administrator implement?

- A. Snapshots
- B. Sandboxing
- C. Patch management
- D. Intrusion detection system

Answer: C

Explanation:

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

QUESTION NO: 757

Which of the following is the term for a fix for a known software problem?

- A. Skiff
- B. Patch
- C. Slipstream
- D. Upgrade

Answer: B

Explanation:

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities.

QUESTION NO: 758

Which of the following practices is used to mitigate a known security vulnerability?

- A. Application fuzzing
- B. Patch management
- C. Password cracking
- D. Auditing security logs

Answer: B

Explanation:

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from new attacks and vulnerabilities that have recently become known.

QUESTION NO: 759

Which of the following can a security administrator implement on mobile devices that will help prevent unwanted people from viewing the data if the device is left unattended?

- A. Screen lock
- B. Voice encryption
- C. GPS tracking
- D. Device encryption

Answer: A

Explanation:

Screen-lock is a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

QUESTION NO: 760

Which of the following can be used on a smartphone to BEST protect against sensitive data loss if the device is stolen? (Select TWO).

- A. Tethering
- B. Screen lock PIN
- C. Remote wipe
- D. Email password
- E. GPS tracking
- F. Device encryption

Answer: C,F

Explanation:

C: Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

F: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

QUESTION NO: 761

Which of the following controls can be implemented together to prevent data loss in the event of theft of a mobile device storing sensitive information? (Select TWO).

- A. Full device encryption
- B. Screen locks
- C. GPS
- D. Asset tracking
- E. Inventory control

Answer: A,B

Explanation:

A: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

B: Screen locks are a security feature that requires the user to enter a PIN or a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

QUESTION NO: 762

A way to assure data at-rest is secure even in the event of loss or theft is to use:

- A. Full device encryption.
- B. Special permissions on the file system.
- C. Trusted Platform Module integration.
- D. Access Control Lists.

Answer: A

Explanation:

Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

QUESTION NO: 763

Which of the following should Matt, a security administrator, include when encrypting smartphones? (Select TWO).

- A. Steganography images
- B. Internal memory
- C. Master boot records
- D. Removable memory cards
- E. Public keys

Answer: B,D

Explanation:

All useable data on the device should be encrypted. This data can be located on the hard drive, or removable drives, such as USB devices and memory cards, and on internal memory.

QUESTION NO: 764

A bank has recently deployed mobile tablets to all loan officers for use at customer sites. Which of the following would BEST prevent the disclosure of customer data in the event that a tablet is lost or stolen?

- A. Application control
- B. Remote wiping
- C. GPS
- D. Screen-locks

Answer: B

Explanation:

Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

QUESTION NO: 765

A small company has recently purchased cell phones for managers to use while working outside if the office.

The company does not currently have a budget for mobile device management and is primarily concerned with deterring leaks if sensitive information obtained by unauthorized access to unattended phones. Which of the following would provide the solution BEST meets the company's requirements?

- A. Screen-lock
- B. Disable removable storage
- C. Full device encryption
- D. Remote wiping

Answer: A

Explanation: Explanation

Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

QUESTION NO: 766

Pete, the system administrator, has concerns regarding users losing their company provided

smartphones. Pete's focus is on equipment recovery. Which of the following BEST addresses his concerns?

- A. Enforce device passwords.
- B. Use remote sanitation.
- C. Enable GPS tracking.
- D. Encrypt stored data.

Answer: C

Explanation:

Global Positioning System (GPS) tracking can be used to identify its location of a stolen device and can allow authorities to recover the device. However, for GPS tracking to work, the device must have an Internet connection or a wireless phone service over which to send its location information.

QUESTION NO: 767

After a security incident involving a physical asset, which of the following should be done at the beginning?

- A. Record every person who was in possession of assets, continuing post-incident.
- B. Create working images of data in the following order: hard drive then RAM.
- C. Back up storage devices so work can be performed on the devices immediately.
- D. Write a report detailing the incident and mitigation suggestions.

Answer: A

Explanation:

Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user.

QUESTION NO: 768

The chief Risk officer is concerned about the new employee BYOD device policy and has requested the security department implement mobile security controls to protect corporate data in the event that a device is lost or stolen. The level of protection must not be compromised even if the communication SIM is removed from the device. Which of the following BEST meets the requirements? (Select TWO)

- A. Asset tracking
- B. Screen-locks

- C. GEO-Tracking
- D. Device encryption

Answer: A,D

Explanation:

A: Asset tracking is the process of maintaining oversight over inventory, and ensuring that a device is still in the possession of the assigned authorized user.

D: Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

QUESTION NO: 769

Which of the following technical controls helps to prevent Smartphones from connecting to a corporate network?

- A. Application white listing
- B. Remote wiping
- C. Acceptable use policy
- D. Mobile device management

Answer: D

Explanation:

Mobile device management (MDM) is allows for managing the mobile devices that employees use to access company resources. MDM is intended to improve security, provide monitoring, enable remote management, and support troubleshooting. It can be used to push or remove applications, manage data, and enforce configuration settings on these devices.

QUESTION NO: 770

Jane, an IT security technician, needs to create a way to secure company mobile devices. Which of the following BEST meets this need?

- A. Implement voice encryption, pop-up blockers, and host-based firewalls.
- B. Implement firewalls, network access control, and strong passwords.
- C. Implement screen locks, device encryption, and remote wipe capabilities.
- D. Implement application patch management, antivirus, and locking cabinets.

Answer: C

Explanation: Screen-lock is a security feature that requires the user to enter a password after a short period of inactivity before they can access the system again. This feature ensures that if your

device is left unattended or is lost or stolen, it will be difficult for anyone else to access your data or applications.

Device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

Remote wipe is the process of deleting data on a device in the event that the device is stolen. This is performed over remote connections such as the mobile phone service or the internet connection and helps ensure that sensitive data is not accessed by unauthorized people.

QUESTION NO: 771

Allowing unauthorized removable devices to connect to computers increases the risk of which of the following?

- A. Data leakage prevention
- B. Data exfiltration
- C. Data classification
- D. Data deduplication

Answer: B

Explanation: Data exfiltration is the unauthorized copying, transfer or retrieval of data from a system.

QUESTION NO: 772

The marketing department wants to distribute pens with embedded USB drives to clients. In the past this client has been victimized by social engineering attacks which led to a loss of sensitive data. The security administrator advises the marketing department not to distribute the USB pens due to which of the following?

- A. The risks associated with the large capacity of USB drives and their concealable nature
- B. The security costs associated with securing the USB drives over time
- C. The cost associated with distributing a large volume of the USB pens
- D. The security risks associated with combining USB drives and cell phones on a network

Answer: A

Explanation:

USB drive and other USB devices represent a security risk as they can be used to either bring malicious code into a secure system or to copy and remove sensitive data out of the system.

QUESTION NO: 773

Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which of the following mitigation techniques would address this concern? (Select TWO).

- A. Disable the USB root hub within the OS.
- B. Install anti-virus software on the USB drives.
- C. Disable USB within the workstations BIOS.
- D. Apply the concept of least privilege to USB devices.
- E. Run spyware detection against all workstations.

Answer: A,C

Explanation:

A: The USB root hub can be disabled from within the operating system.

C: USB can also be configured and disabled in the system BIOS.

QUESTION NO: 774

A company has purchased an application that integrates into their enterprise user directory for account authentication. Users are still prompted to type in their usernames and passwords. Which of the following types of authentication is being utilized here?

- A. Separation of duties
- B. Least privilege
- C. Same sign-on
- D. Single sign-on

Answer: C

Explanation: Same sign-on requires the users to re-enter their credentials but it allows them to use the same credentials that they use to sign on locally.

QUESTION NO: 775

Prior to leaving for an extended vacation, Joe uses his mobile phone to take a picture of his family in the house living room. Joe posts the picture on a popular social media site together with the message: "Heading to our two weeks vacation to Italy." Upon returning home, Joe discovers that the house was burglarized. Which of the following is the MOST likely reason the house was

burglarized if nobody knew Joe's home address?

- A. Joe has enabled the device access control feature on his mobile phone.
- B. Joe's home address can be easily found using the TRACEROUTE command.
- C. The picture uploaded to the social media site was geo-tagged by the mobile phone.
- D. The message posted on the social media site informs everyone the house will be empty.

Answer: C

Explanation:

Geo-tagging is the process of embedding the GPS coordinates in image files and images taken using a smartphone or a digital camera. The geotagged information accompanying the image allows anyone to discover the precise location where the image was taken.

QUESTION NO: 776

The call center supervisor has reported that many employees have been playing preinstalled games on company computers and this is reducing productivity.

Which of the following would be MOST effective for preventing this behavior?

- A. Acceptable use policies
- B. Host-based firewalls
- C. Content inspection
- D. Application whitelisting

Answer: D

Explanation:

Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list.

QUESTION NO: 777

Which of the following would prevent a user from installing a program on a company-owned mobile device?

- A. White-listing
- B. Access control lists
- C. Geotagging
- D. Remote wipe

Answer: A

Explanation:

Application whitelisting is a form of application security which prevents any software from running on a system unless it is included on a preapproved exception list.

QUESTION NO: 778

If Organization A trusts Organization B and Organization B trusts Organization C, then Organization A trusts Organization C. Which of the following PKI concepts is this describing?

- A. Transitive trust
- B. Public key trust
- C. Certificate authority trust
- D. Domain level trust

Answer: A

Explanation:

In transitive trusts, trust between a first party and a third party flows through a second party that is trusted by both the first party and the third party.

QUESTION NO: 779

Which of the following can be performed when an element of the company policy cannot be enforced by technical means?

- A. Develop a set of standards
- B. Separation of duties
- C. Develop a privacy policy
- D. User training

Answer: D

Explanation:

User training is an important aspect of maintaining safety and security. It helps improve users' security awareness in terms of prevention, enforcement, and threats. It is of critical importance when element of the company policy cannot be enforced by technical means.

QUESTION NO: 780

Which of the following file systems is from Microsoft and was included with their earliest operating systems?

- A. NTFS
- B. UFS
- C. MTFS
- D. FAT

Answer: D

Explanation:

File Allocation Table (FAT) is a file system created by Microsoft and used for its earliest DOS operating systems.

QUESTION NO: 781

An IT security technician needs to establish host based security for company workstations. Which of the following will BEST meet this requirement?

- A. Implement IIS hardening by restricting service accounts.
- B. Implement database hardening by applying vendor guidelines.
- C. Implement perimeter firewall rules to restrict access.
- D. Implement OS hardening by applying GPOs.

Answer: D

Explanation: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services. This can be implemented using the native security features of an operating system, such as Group Policy Objects (GPOs).

QUESTION NO: 782

Disabling unnecessary services, restricting administrative access, and enabling auditing controls on a server are forms of which of the following?

- A. Application patch management
- B. Cross-site scripting prevention
- C. Creating a security baseline
- D. System hardening

Answer: D

Explanation:

Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

QUESTION NO: 783

A network administrator noticed various chain messages have been received by the company.

Which of the following security controls would need to be implemented to mitigate this issue?

- A. Anti-spam
- B. Antivirus
- C. Host-based firewalls
- D. Anti-spyware

Answer: A

Explanation: A spam filter is a software or hardware solution used to identify and block, filter, or remove unwanted messages sent via email or instant messaging (IM).

QUESTION NO: 784

Which of the following will allow Pete, a security analyst, to trigger a security alert because of a tracking cookie?

- A. Network based firewall
- B. Anti-spam software
- C. Host based firewall
- D. Anti-spyware software

Answer: D

Explanation:

Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie.

QUESTION NO: 785

A security administrator wants to deploy security controls to mitigate the threat of company employees' personal information being captured online. Which of the following would BEST serve this purpose?

- A. Anti-spyware
- B. Antivirus
- C. Host-based firewall
- D. Web content filter

Answer: A

Explanation:

Spyware monitors a user's activity and uses network protocols to reports it to a third party without the user's knowledge. This is usually accomplished using a tracking cookie.

QUESTION NO: 786

A user has several random browser windows opening on their computer. Which of the following programs can be installed on his machine to help prevent this from happening?

- A. Antivirus
- B. Pop-up blocker
- C. Spyware blocker
- D. Anti-spam

Answer: B

Explanation:

Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code.

QUESTION NO: 787

Which of the following is a vulnerability associated with disabling pop-up blockers?

- A. An alert message from the administrator may not be visible
- B. A form submitted by the user may not open
- C. The help window may not be displayed
- D. Another browser instance may execute malicious code

Answer: D

Explanation: Pop-up blockers prevent websites from opening new browser windows without the users consent. These are often used for advertisements but can also be used to distribute malicious code.

QUESTION NO: 788

Which of the following encompasses application patch management?

- A. Configuration management
- B. Policy management
- C. Cross-site request forgery
- D. Fuzzing

Answer: A

Explanation:

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system first to ensure that the updates do not have detrimental effects on the system and its configuration, and, should the updates have no detrimental effects on the test systems, backing up the production systems before applying the updates on a production system.

QUESTION NO: 789

A periodic update that corrects problems in one version of a product is called a

- A. Hotfix
- B. Overhaul
- C. Service pack
- D. Security update

Answer: C

Explanation:

A service pack is a collection of updates and hotfixes that address a number of software issues, as well as new software features. It is released periodically by the vendor.

QUESTION NO: 790

A technician has implemented a system in which all workstations on the network will receive security updates on the same schedule. Which of the following concepts does this illustrate?

- A. Patch management
- B. Application hardening
- C. White box testing
- D. Black box testing

Answer: A

Explanation:

Patch management is the process of maintaining the latest source code for applications and operating systems by applying the latest vendor updates. This helps protect a systems from newly discovered attacks and vulnerabilities. A part of patch management is testing the effects of vendor updates on a test system before applying the updates on a production system, and scheduling updates.

QUESTION NO: 791

Pete, the compliance manager, wants to meet regulations. Pete would like certain ports blocked only on all computers that do credit card transactions. Which of the following should Pete implement to BEST achieve this goal?

- A. A host-based intrusion prevention system
- B. A host-based firewall
- C. Antivirus update system
- D. A network-based intrusion detection system

Answer: B

Explanation:

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet.

QUESTION NO: 792

Each server on a subnet is configured to only allow SSH access from the administrator's workstation. Which of the following BEST describes this implementation?

- A. Host-based firewalls

- B. Network firewalls
- C. Network proxy
- D. Host intrusion prevention

Answer: A

Explanation:

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system.

QUESTION NO: 793

Which of the following is an important step in the initial stages of deploying a host-based firewall?

- A. Selecting identification versus authentication
- B. Determining the list of exceptions
- C. Choosing an encryption algorithm
- D. Setting time of day restrictions

Answer: B

Explanation:

A host-based firewall is installed on a client system and is used to protect the client system from the activities of the user as well as from communication from the network or Internet. These firewalls manage network traffic using filters to block certain ports and protocols while allowing others to pass through the system.

QUESTION NO: 794

Which of the following MOST interferes with network-based detection techniques?

- A. Mime-encoding
- B. SSL
- C. FTP
- D. Anonymous email accounts

Answer: B

Explanation:

Secure Sockets Layer (SSL) is used to establish secure TCP communication between two machines by encrypting the communication. Encrypted communications cannot easily be

inspected for anomalies by network-based intrusion detection systems (NIDS).

QUESTION NO: 795

Joe, a network security engineer, has visibility to network traffic through network monitoring tools.

However, he's concerned that a disgruntled employee may be targeting a server containing the company's financial records. Which of the following security mechanism would be MOST appropriate to confirm Joe's suspicion?

- A. HIDS
- B. HIPS
- C. NIPS
- D. NIDS

Answer: A

Explanation:

A host-based IDS (HIDS) is an intrusion detection system that runs as a service on a host computer system. It is used to monitor the machine logs, system events, and application activity for signs of intrusion. It is useful for detecting attacks that originate outside the organization as well as attacks by internal users logged on to the system.

QUESTION NO: 796

Which of the following devices will help prevent a laptop from being removed from a certain location?

- A. Device encryption
- B. Cable locks
- C. GPS tracking
- D. Remote data wipes

Answer: B

Explanation:

Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep smaller devices from being easy to steal.

QUESTION NO: 797

Which of the following can be used as an equipment theft deterrent?

- A. Screen locks
- B. GPS tracking
- C. Cable locks
- D. Whole disk encryption

Answer: C

Explanation:

Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep smaller devices from being easy to steal.

QUESTION NO: 798

The librarian wants to secure the public Internet kiosk PCs at the back of the library. Which of the following would be the MOST appropriate? (Select TWO).

- A. Device encryption
- B. Antivirus
- C. Privacy screen
- D. Cable locks
- E. Remote wipe

Answer: B,D

Explanation:

B: Antivirus software is used to protect systems against viruses, which are a form of malicious code designed to spread from one system to another, consuming network resources. Public systems are particularly prone to viruses.

D: Cable locks are theft deterrent devices that can be used to tether a device to a fixed point keep devices from being easy to steal.

QUESTION NO: 799

A computer is suspected of being compromised by malware. The security analyst examines the computer and finds that a service called Telnet is running and connecting to an external website over port 443. This Telnet service was found by comparing the system's services to the list of standard services on the company's system image. This review process depends on:

- A. MAC filtering.
- B. System hardening.
- C. Rogue machine detection.
- D. Baselineing.

Answer: D

Explanation:

Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

QUESTION NO: 800

Identifying a list of all approved software on a system is a step in which of the following practices?

- A. Passively testing security controls
- B. Application hardening
- C. Host software baselining
- D. Client-side targeting

Answer: C

Explanation:

Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

QUESTION NO: 801

A new application needs to be deployed on a virtual server. The virtual server hosts a SQL server that is used by several employees.

Which of the following is the BEST approach for implementation of the new application on the virtual server?

- A. Take a snapshot of the virtual server after installing the new application and store the snapshot

in a secure location.

B. Generate a baseline report detailing all installed applications on the virtualized server after installing the new application.

C. Take a snapshot of the virtual server before installing the new application and store the snapshot in a secure location.

D. Create an exact copy of the virtual server and store the copy on an external hard drive after installing the new application.

Answer: C

Explanation:

Snapshots are backups of virtual machines that can be used to quickly recover from poor updates, and errors arising from newly installed applications. However, the snapshot should be taken before the application or update is installed.

QUESTION NO: 802

The information security technician wants to ensure security controls are deployed and functioning as intended to be able to maintain an appropriate security posture. Which of the following security techniques is MOST appropriate to do this?

A. Log audits

B. System hardening

C. Use IPS/IDS

D. Continuous security monitoring

Answer: D

Explanation:

A security baseline is the security setting of a system that is known to be secure. This is the initial security setting of a system. Once the baseline has been applied, it must be maintained or improved. Maintaining the security baseline requires continuous monitoring.

QUESTION NO: 803

Which of the following solutions provides the most flexibility when testing new security controls prior to implementation?

A. Trusted OS

B. Host software baselining

C. OS hardening

D. Virtualization

Answer: D

Explanation:

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

QUESTION NO: 804

A company is about to release a very large patch to its customers. An administrator is required to test patch installations several times prior to distributing them to customer PCs.

Which of the following should the administrator use to test the patching process quickly and often?

- A.** Create an incremental backup of an unpatched PC
- B.** Create an image of a patched PC and replicate it to servers
- C.** Create a full disk image to restore after each installation
- D.** Create a virtualized sandbox and utilize snapshots

Answer: D

Explanation:

Sandboxing is the process of isolating a system before installing new applications or patches on it so as to restrict the software from being able to cause harm to production systems.

Before the patch is installed, a snapshot of the system should be taken. Snapshots are backups that can be used to quickly recover from poor updates, and errors arising from newly installed applications.

QUESTION NO: 805

An administrator is building a development environment and requests that three virtual servers are cloned and placed in a new virtual network isolated from the production network. Which of the following describes the environment the administrator is building?

- A.** Cloud
- B.** Trusted
- C.** Sandbox
- D.** Snapshot

Answer: C

Explanation:

Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems.

QUESTION NO: 806

Which of the following techniques describes the use of application isolation during execution to prevent system compromise if the application is compromised?

- A. Least privilege
- B. Sandboxing
- C. Black box
- D. Application hardening

Answer: B

Explanation:

Sandboxing is the process of isolating a system before installing new applications on it so as to restrict any potential malware that may be embedded in the new application from being able to cause harm to production systems.

QUESTION NO: 807

Which of the following can be used to maintain a higher level of security in a SAN by allowing isolation of mis-configurations or faults?

- A. VLAN
- B. Protocol security
- C. Port security
- D. VSAN

Answer: D

Explanation:

A storage area network (SAN) is a secondary network that offers storage isolation by consolidating storage devices such as hard drives, drive arrays, optical jukeboxes, and tape libraries.

Virtualization can be used to further enhance the security of a SAN by using switches to create a VSAN. These switches act as routers controlling and filtering traffic into and out of the VSAN while allowing unrestricted traffic within the VSAN.

QUESTION NO: 808

A company needs to receive data that contains personally identifiable information. The company requires both the transmission and data at rest to be encrypted. Which of the following achieves this goal? (Select TWO).

- A. SSH
- B. TFTP
- C. NTLM
- D. TKIP
- E. SMTP
- F. PGP/GPG

Answer: A,F

Explanation:

We can use SSH to encrypt the transmission and PGP/GPG to encrypt the data at rest (on disk).

A: Secure Shell (SSH) is a cryptographic protocol that can be used to secure network communication. It establishes a secure tunnel over an insecure network.

F: Pretty Good Privacy (PGP) is a data encryption and decryption solution that can be used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

QUESTION NO: 809

Which of the following does full disk encryption prevent?

- A. Client side attacks
- B. Clear text access
- C. Database theft
- D. Network-based attacks

Answer: B

Explanation:

Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

QUESTION NO: 810

Full disk encryption is MOST effective against which of the following threats?

- A. Denial of service by data destruction
- B. Eavesdropping emanations
- C. Malicious code
- D. Theft of hardware

Answer: D

Explanation:

Full-disk encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. However, it does not prevent the theft of hardware it only protects data should the device be stolen.

QUESTION NO: 811

Which of the following is the BEST method for ensuring all files and folders are encrypted on all corporate laptops where the file structures are unknown?

- A. Folder encryption
- B. File encryption
- C. Whole disk encryption
- D. Steganography

Answer: C

Explanation:

Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen. Furthermore, full-disk encryption is not dependant on knowledge of the file structure.

QUESTION NO: 812

To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

- A. Full disk encryption
- B. Application isolation
- C. Digital rights management
- D. Data execution prevention

Answer: A

Explanation:

Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen.

QUESTION NO: 813

A merchant acquirer has the need to store credit card numbers in a transactional database in a high performance environment. Which of the following BEST protects the credit card data?

- A. Database field encryption
- B. File-level encryption
- C. Data loss prevention system
- D. Full disk encryption

Answer: A

Explanation:

Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the data base. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field.

QUESTION NO: 814

Which of the following types of data encryption would Matt, a security administrator, use to encrypt a specific table?

- A. Full disk
- B. Individual files
- C. Database
- D. Removable media

Answer: C

Explanation:

A table is stored in a database. Database encryption makes use of cryptography functions that are built into the database software to encrypt the data stored in the database. This often offers granular encryption options which allows for the encryptions of the entire database, specific database tables, or specific database fields, such as a credit card number field.

QUESTION NO: 815

A database administrator would like to start encrypting database exports stored on the SAN, but the storage administrator warns that this may drastically increase the amount of disk space used by the exports. Which of the following explains the reason for the increase in disk space usage?

- A. Deduplication is not compatible with encryption
- B. The exports are being stored on smaller SAS drives
- C. Encrypted files are much larger than unencrypted files
- D. The SAN already uses encryption at rest

Answer: C

Explanation:

Encryption adds overhead to the data which results in an increase in file size. This overhead is attached to each file and could include the encryption/decryption key, data recovery files and data decryption field in file header. As a result, requires increased storage space.

QUESTION NO: 816

Which of the following is an advantage of implementing individual file encryption on a hard drive which already deploys full disk encryption?

- A. Reduces processing overhead required to access the encrypted files
- B. Double encryption causes the individually encrypted files to partially lose their properties
- C. Individually encrypted files will remain encrypted when copied to external media
- D. File level access control only apply to individually encrypted files in a fully encrypted drive

Answer: C

Explanation:

With full disk encryption a file is encrypted as long as it remains on the disk. This is because the data on the disk is decrypted when the user logs on, thus the data is in a decrypted form when it is copied to another disk. Individually encrypted files on the other hand remain encrypted.

QUESTION NO: 817

A team of firewall administrators have access to a `master password list' containing service account passwords. Which of the following BEST protects the master password list?

- A. File encryption
- B. Password hashing
- C. USB encryption
- D. Full disk encryption

Answer: A

Explanation:

File encryption can be used to protect the contents of individual files. It uses randomly generated symmetric encryption keys for the file and stores the key in an encrypted form using the user's public key on the encrypted file.

QUESTION NO: 818

A security administrator has concerns regarding employees saving data on company provided mobile devices. Which of the following would BEST address the administrator's concerns?

- A. Install a mobile application that tracks read and write functions on the device.
- B. Create a company policy prohibiting the use of mobile devices for personal use.
- C. Enable GPS functionality to track the location of the mobile devices.
- D. Configure the devices so that removable media use is disabled.

Answer: D

Explanation:

Mobile devices can be plugged into computers where they appear as an additional disk in the same way as a USB drive. This is known as removable media. This would enable users to copy company data onto the mobile devices. By disabling removable media use, the users will not be able to copy data onto the mobile devices.

QUESTION NO: 819

Which of the following can be used to mitigate risk if a mobile device is lost?

- A. Cable lock
- B. Transport encryption
- C. Voice encryption

D. Strong passwords

Answer: D

Explanation:

Passwords are the most likely mechanism that can be used to mitigate risk when a mobile device is lost. A strong password would be more difficult to crack.

QUESTION NO: 820

Which of the following types of encryption will help in protecting files on a PED?

- A. Mobile device encryption**
- B. Transport layer encryption**
- C. Encrypted hidden container**
- D. Database encryption**

Answer: A

Explanation:

Device encryption encrypts the data on a Personal Electronic Device (PED). This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

QUESTION NO: 821

Which of the following is a way to implement a technical control to mitigate data loss in case of a mobile device theft?

- A. Disk encryption**
- B. Encryption policy**
- C. Solid state drive**
- D. Mobile device policy**

Answer: A

Explanation:

Disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

QUESTION NO: 822

An SSL/TLS private key is installed on a corporate web proxy in order to inspect HTTPS requests.

Which of the following describes how this private key should be stored so that it is protected from theft?

- A. Implement full disk encryption
- B. Store on encrypted removable media
- C. Utilize a hardware security module
- D. Store on web proxy file system

Answer: C

Explanation:

Hardware Security Module (HSM) hardware-based encryption solution that is usually used in conjunction with PKI to enhance security with certification authorities (CAs). It is available as an expansion card and can cryptographic keys, passwords, or certificates.

QUESTION NO: 823

Which of the following has a storage root key?

- A. HSM
- B. EFS
- C. TPM
- D. TKIP

Answer: C

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates on non-volatile (NV) memory. Data stored on NV memory is retained unaltered when the device has no power. The storage root key is embedded in the TPM to protect TPM keys created by applications, so that these keys cannot be used without the TPM.

QUESTION NO: 824

Which of the following would be used when a higher level of security is desired for encryption key storage?

- A. TACACS+
- B. L2TP

- C. LDAP
- D. TPM

Answer: D

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 825

Which of the following is a hardware based encryption device?

- A. EFS
- B. TrueCrypt
- C. TPM
- D. SLE

Answer: C

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 826

A company wants to ensure that all aspects of data are protected when sending to other sites within the enterprise. Which of the following would ensure some type of encryption is performed while data is in transit?

- A. SSH
- B. SHA1
- C. TPM
- D. MD5

Answer: C

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 827

Which of the following should be enabled in a laptop's BIOS prior to full disk encryption?

- A. USB
- B. HSM
- C. RAID
- D. TPM

Answer: D

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 828

Which of the following is a hardware-based security technology included in a computer?

- A. Symmetric key
- B. Asymmetric key
- C. Whole disk encryption
- D. Trusted platform module

Answer: D

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 829

Which of the following provides dedicated hardware-based cryptographic functions to an operating system and its applications running on laptops and desktops?

- A. TPM

- B. HSM
- C. CPU
- D. FPU

Answer: A

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 830

Which of the following is built into the hardware of most laptops but is not setup for centralized management by default?

- A. Whole disk encryption
- B. TPM encryption
- C. USB encryption
- D. Individual file encryption

Answer: B

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 831

A hospital IT department wanted to secure its doctor's tablets. The IT department wants operating system level security and the ability to secure the data from alteration. Which of the following methods would MOST likely work?

- A. Cloud storage
- B. Removal Media
- C. TPM
- D. Wiping

Answer: C

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the

system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 832

Which of the following hardware-based encryption devices is used as a part of multi-factor authentication to access a secured computing system?

- A. Database encryption
- B. USB encryption
- C. Whole disk encryption
- D. TPM

Answer: D

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 833

The systems administrator wishes to implement a hardware-based encryption method that could also be used to sign code. They can achieve this by:

- A. Utilizing the already present TPM.
- B. Configuring secure application sandboxes.
- C. Enforcing whole disk encryption.
- D. Moving data and applications into the cloud.

Answer: A

Explanation:

Trusted Platform Module (TPM) is a hardware-based encryption solution that is embedded in the system's motherboard and is enabled or disabled in BIOS. It helps with hash key generation and stores cryptographic keys, passwords, or certificates.

QUESTION NO: 834

Which of the following BEST explains the use of an HSM within the company servers?

- A. Thumb drives present a significant threat which is mitigated by HSM.
- B. Software encryption can perform multiple functions required by HSM.
- C. Data loss by removable media can be prevented with DLP.
- D. Hardware encryption is faster than software encryption.

Answer: D

Explanation:

Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. It provides a fast solution for the for large asymmetrical encryption calculations and is much faster than software-based cryptographic solutions.

QUESTION NO: 835

Access mechanisms to data on encrypted USB hard drives must be implemented correctly otherwise:

- A. user accounts may be inadvertently locked out.
- B. data on the USB drive could be corrupted.
- C. data on the hard drive will be vulnerable to log analysis.
- D. the security controls on the USB drive can be bypassed.

Answer: D

Explanation:

A common access mechanism to data on encrypted USB hard drives is a password. If a weak password is used, someone could guess the password and bypass the security controls on the USB drive to access the data.

QUESTION NO: 836

A security administrator has implemented a policy to prevent data loss. Which of the following is the BEST method of enforcement?

- A. Internet networks can be accessed via personally-owned computers.
- B. Data can only be stored on local workstations.
- C. Wi-Fi networks should use WEP encryption by default.
- D. Only USB devices supporting encryption are to be used.

Answer: D

Explanation:

The concern for preventing data loss is the concern for maintaining data confidentiality. This can

be accomplished through encryption, access controls, and steganography.

USB encryption is usually provided by the vendor of the USB device. It is not included on all USB devices.

QUESTION NO: 837

Which of the following data security techniques will allow Matt, an IT security technician, to encrypt a system with speed as its primary consideration?

- A. Hard drive encryption
- B. Infrastructure as a service
- C. Software based encryption
- D. Data loss prevention

Answer: A

Explanation:

Disk and device encryption encrypts the data on the device. This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen. It should be implemented using a hardware-based solution for greater speed.

QUESTION NO: 838

A large corporation has data centers geographically distributed across multiple continents. The company needs to securely transfer large amounts of data between the data center. The data transfer can be accomplished physically or electronically, but must prevent eavesdropping while the data is on transit. Which of the following represents the BEST cryptographic solution?

- A. Driving a van full of Micro SD cards from data center to data center to transfer data
- B. Exchanging VPN keys between each data center via an SSL connection and transferring the data in the VPN
- C. Using a courier to deliver symmetric VPN keys to each data center and transferring data in the VPN
- D. Using PKI to encrypt each file and transferring them via an Internet based FTP or cloud server

Answer: B

Explanation:

A virtual private network (VPN) is an encrypted communication tunnel that connects two systems over an untrusted network, such as the Internet. They provide security for both authentication and data transmission through a process called encapsulation.

Secure Sockets Layer (SSL) can be used to exchange the VPN keys securely. SSL is used to

establish secure TCP communication between two machines by encrypting the communication.

QUESTION NO: 839

A security administrator wants to ensure that the message the administrator sends out to their Chief Financial Officer (CFO) does not get changed in route. Which of the following is the administrator MOST concerned with?

- A. Data confidentiality
- B. High availability
- C. Data integrity
- D. Business continuity

Answer: C

Explanation:

Integrity is the process of ensuring that the information has not been altered during transmission. This can be accomplished by means of hashing.

QUESTION NO: 840

An administrator wants to ensure that the reclaimed space of a hard drive has been sanitized while the computer is in use. Which of the following can be implemented?

- A. Cluster tip wiping
- B. Individual file encryption
- C. Full disk encryption
- D. Storage retention

Answer: A

Explanation:

A computer hard disk is divided into small segments called clusters. A file usually spans several clusters but rarely fills the last cluster, which is called cluster tip. This cluster tip area may contain file data because the size of the file you are working with may grow or shrink and needs to be securely deleted.

QUESTION NO: 841

The act of magnetically erasing all of the data on a disk is known as:

- A. Wiping
- B. Dissolution
- C. Scrubbing
- D. Degaussing

Answer: D

Explanation:

Degaussing is a form of data wiping that entails the use of magnets to alter the magnetic structure of the storage medium.

QUESTION NO: 842

Company XYZ recently salvaged company laptops and removed all hard drives, but the Chief Information Officer (CIO) is concerned about disclosure of confidential information. Which of the following is the MOST secure method to dispose of these hard drives?

- A. Degaussing
- B. Physical Destruction
- C. Lock up hard drives in a secure safe
- D. Wipe

Answer: B

Explanation:

The physical destruction of hard drives is the only secure means of disposing of hard drives. This can include incineration, an acid bath, and crushing.

QUESTION NO: 843

During a recent investigation, an auditor discovered that an engineer's compromised workstation was being used to connect to SCADA systems while the engineer was not logged in. The engineer is responsible for administering the SCADA systems and cannot be blocked from connecting to them. The SCADA systems cannot be modified without vendor approval which requires months of testing.

Which of the following is MOST likely to protect the SCADA systems from misuse?

- A. Update anti-virus definitions on SCADA systems
- B. Audit accounts on the SCADA systems
- C. Install a firewall on the SCADA network
- D. Deploy NIPS at the edge of the SCADA network

Answer: D

Explanation:

A supervisory control and data acquisition (SCADA) system is an industrial control system (ICS) that is used to control infrastructure processes, facility-based processes, or industrial processes. A network-based IPS (NIPS) is an intrusion detection and prevention system that scans network traffic in real time against a database of attack signatures. It is useful for detecting and responding to network-based attacks originating from outside the organization.

QUESTION NO: 844

Which of the following are examples of network segmentation? (Select TWO).

- A. IDS
- B. IaaS
- C. DMZ
- D. Subnet
- E. IPS

Answer: C,D

Explanation:

C: A demilitarized zone (DMZ) is a part of the network that is separated or segmented from the rest of the network by means of firewalls and acts as a buffer between the untrusted public Internet and the trusted local area network (LAN).

D: IP subnets can be used to separate or segment networks while allowing communication between the network segments via routers.

QUESTION NO: 845

Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

- A. Intrusion Detection System
- B. Flood Guard Protection
- C. Web Application Firewall
- D. URL Content Filter

Answer: C

Explanation:

Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an

attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity.

QUESTION NO: 846

When considering a vendor-specific vulnerability in critical industrial control systems which of the following techniques supports availability?

- A. Deploying identical application firewalls at the border
- B. Incorporating diversity into redundant design
- C. Enforcing application white lists on the support workstations
- D. Ensuring the systems' anti-virus definitions are up-to-date

Answer: B

Explanation:

If you know there is a vulnerability that is specific to one vendor, you can improve availability by implementing multiple systems that include at least one system from a different vendor and so is not affected by the vulnerability.

QUESTION NO: 847

Which of the following devices would be the MOST efficient way to filter external websites for staff on an internal network?

- A. Protocol analyzer
- B. Switch
- C. Proxy
- D. Router

Answer: C

Explanation:

A proxy is a device that acts on behalf of other devices. All internal user communications with the Internet could be controlled through a proxy server, which can be configured to automatically filter out or block certain sites and content. It can also cache often-accessed sites to improve performance.

QUESTION NO: 848

A Human Resources user is issued a virtual desktop typically assigned to Accounting employees. A system administrator wants to disable certain services and remove the local accounting groups installed by default on this virtual machine. The system administrator is adhering to which of the following security best practices?

- A. Black listing applications
- B. Operating System hardening
- C. Mandatory Access Control
- D. Patch Management

Answer: B

Explanation:

Operating System hardening is the process of securing the operating system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing unnecessary functions and features, removing unnecessary usernames or logins and disabling unnecessary services.

QUESTION NO: 849

A security administrator wants to implement a solution which will allow some applications to run under the user's home directory and only have access to files stored within the same user's folder, while other applications have access to shared folders. Which of the following BEST addresses these requirements if the environment is concurrently shared by multiple users?

- A. OS Virtualization
- B. Trusted OS
- C. Process sandboxing
- D. File permission

Answer: C

Explanation:

Sandboxing involves running applications in restricted memory areas. It limits the possibility of an application crash, allowing a user to access another application or the data associated with it.

QUESTION NO: 850

Which of the following should a company implement to BEST mitigate from zero-day malicious code executing on employees' computers?

- A. Least privilege accounts
- B. Host-based firewalls
- C. Intrusion Detection Systems
- D. Application white listing

Answer: D

Explanation:

Application whitelisting is a security stance that prohibits unauthorized software from being able to execute unless it is on the preapproved exception list: the whitelist. This prevents any and all software, including malware, from executing unless it is on the whitelist. This can help block zero-day attacks, which are new attacks that exploit flaws or vulnerabilities in targeted systems and applications that are unknown or undisclosed to the world in general.

QUESTION NO: 851

Which of the following is a control that allows a mobile application to access and manipulate information which should only be available by another application on the same mobile device (e.g. a music application posting the name of the current song playing on the device on a social media site)?

- A. Co-hosted application
- B. Transitive trust
- C. Mutually exclusive access
- D. Dual authentication

Answer: B

Explanation:

Transitive trust is a form of trust that flows from one entity to another so that if A trusts B and B trusts C, A automatically trusts C.

QUESTION NO: 852

Joe, a technician, is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

- A. OS hardening
- B. Application control
- C. Virtualization

D. Sandboxing

Answer: C

Explanation:

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware, reducing costs. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

QUESTION NO: 853

Establishing a method to erase or clear cluster tips is an example of securing which of the following?

- A. Data in transit**
- B. Data at rest**
- C. Data in use**
- D. Data in motion**

Answer: B

Explanation:

A computer hard disk is divided into small segments called clusters. A file stored on a hard disk usually spans several clusters but rarely fills the last cluster, which is called cluster tip. This cluster tip area may contain file data because the size of the file you are working with may grow or shrink and needs to be securely deleted. Data stored on the hard drive is called data at rest.

QUESTION NO: 854

An application developer has tested some of the known exploits within a new application. Which of the following should the administrator utilize to test for unidentified faults or memory leaks?

- A. XSRF Attacks**
- B. Fuzzing**
- C. Input Validations**
- D. SQL Injections**

Answer: B

Explanation:

Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

QUESTION NO: 855

Which of the following controls should critical application servers implement to protect themselves from other potentially compromised application services?

- A. NIPS
- B. Content filter
- C. NIDS
- D. Host-based firewalls

Answer: D

Explanation:

A host-based firewall is designed to protect the host from network based attack by using filters to limit the network traffic that is allowed to enter or leave the host. The action of a filter is to allow, deny, or log the network packet. Allow enables the packet to continue toward its destination. Deny blocks the packet from going any further and effectively discarding it. Log records information about the packet into a log file. Filters can be based on protocol and ports. By blocking protocols and ports that are not required, other potentially compromised application services would be prevented from being exploited across the network.

QUESTION NO: 856

Which of the following would be MOST appropriate if an organization's requirements mandate complete control over the data and applications stored in the cloud?

- A. Hybrid cloud
- B. Community cloud
- C. Private cloud
- D. Public cloud

Answer: C

Explanation:

A private cloud is a cloud service for internal use only and is located within a corporate network rather than on the Internet. It is usually owned, managed, and operated by the company, which gives the company full control over the data and applications stored in the cloud.

QUESTION NO: 857

It has been discovered that students are using kiosk tablets intended for registration and scheduling to play games and utilize instant messaging. Which of the following could BEST eliminate this issue?

- A. Device encryption
- B. Application control
- C. Content filtering
- D. Screen-locks

Answer: B

Explanation:

Application control is the process of controlling what applications are installed on a device. This may reduce exposure to malicious software by limiting the user's ability to install applications that come from unknown sources or have no work-related features.

QUESTION NO: 858

Verifying the integrity of data submitted to a computer program at or during run-time, with the intent of preventing the malicious exploitation of unintentional effects in the structure of the code, is BEST described as which of the following?

- A. Output sanitization
- B. Input validation
- C. Application hardening
- D. Fuzzing

Answer: B

Explanation:

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

QUESTION NO: 859

Which of the following is a security advantage of using NoSQL vs. SQL databases in a three-tier environment?

- A. NoSQL databases are not vulnerable to XSRF attacks from the application server.
- B. NoSQL databases are not vulnerable to SQL injection attacks.
- C. NoSQL databases encrypt sensitive information by default.
- D. NoSQL databases perform faster than SQL databases on the same hardware.

Answer: B

Explanation:

NoSQL is a nonrelational database and does not use SQL. It is therefore not vulnerable to SQL injection attacks but is vulnerable to similar injection-type attacks.

QUESTION NO: 860 DRAG DROP

A security administrator is given the security and availability profiles for servers that are being deployed.

Match each RAID type with the correct configuration and MINIMUM number of drives.

Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

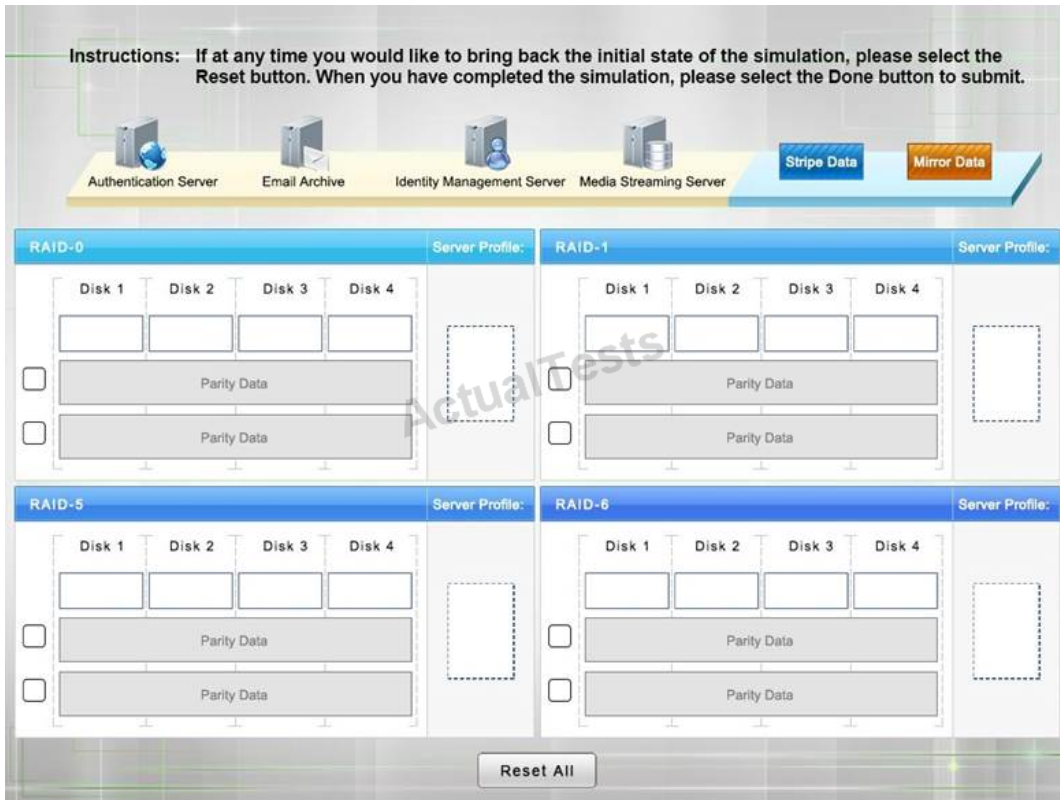
All drive definitions can be dragged as many times as necessary

Not all placeholders may be filled in the RAID configuration boxes

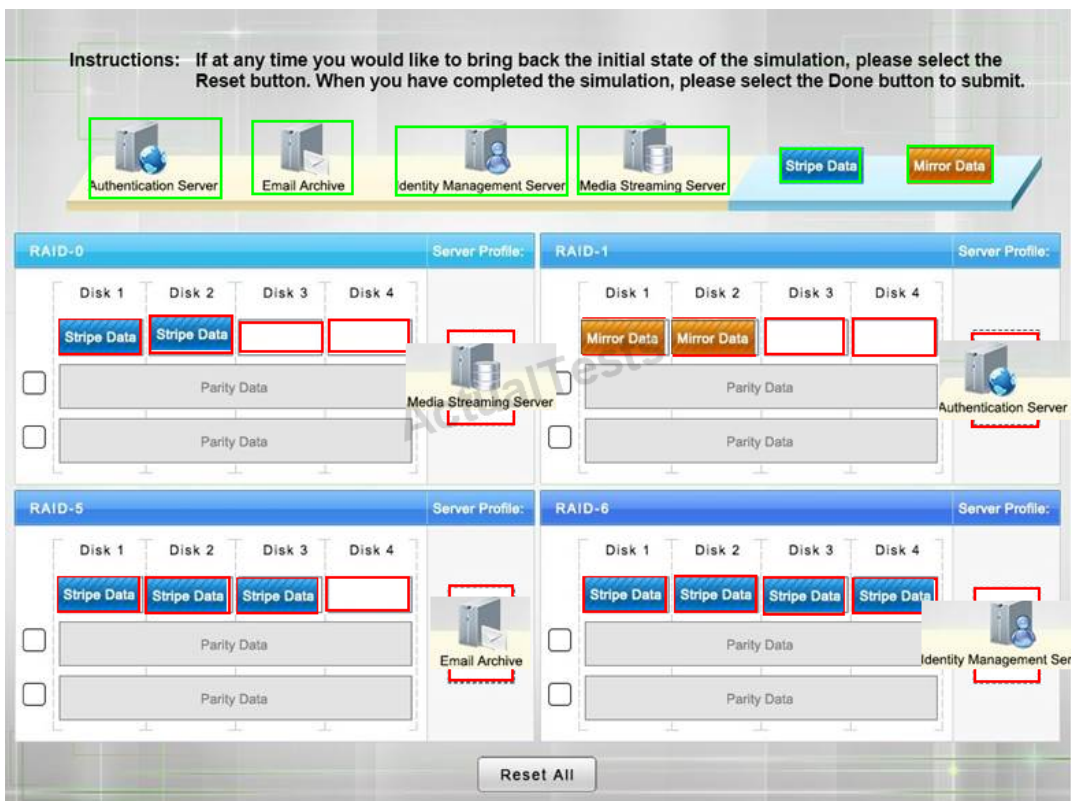
If parity is required, please select the appropriate number of parity checkboxes

Server profiles may be dragged only once

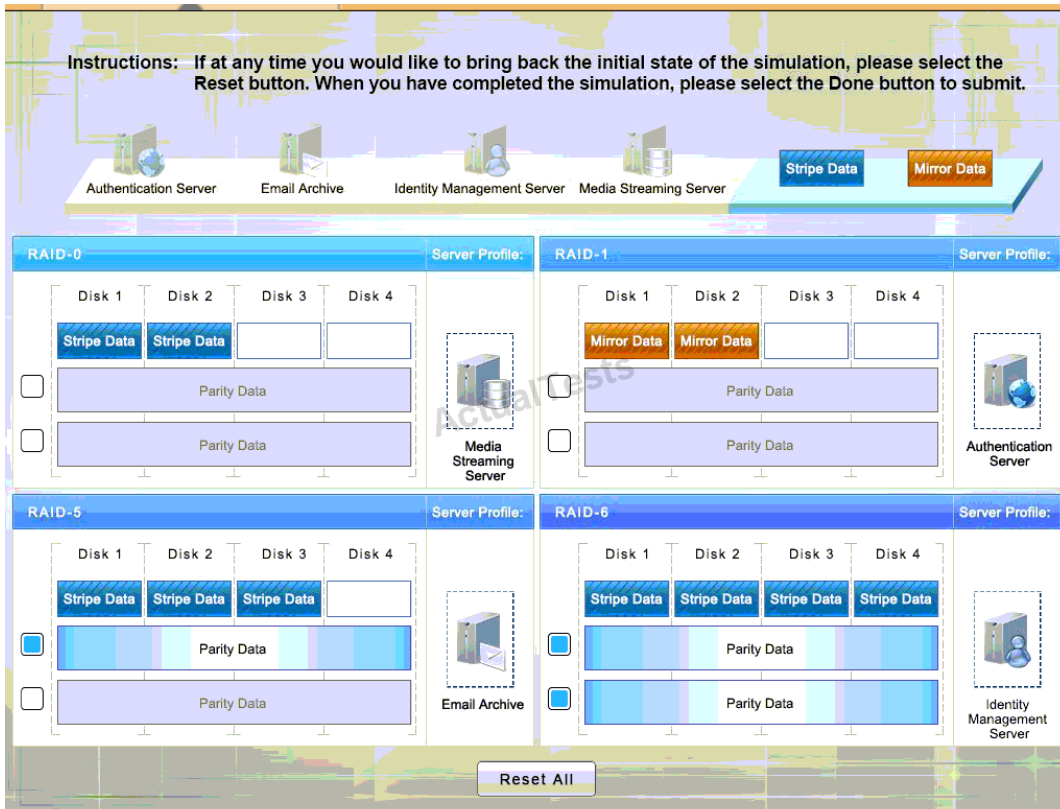
Instructions: If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.



Answer:



Explanation:



RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity. RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.

RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server.

RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a single disk failure. RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 34-36, 234-235

Topic 5, Access Control and Identity Management

QUESTION NO: 861

Jane, a security administrator, needs to implement a secure wireless authentication method that uses a remote RADIUS server for authentication.

Which of the following is an authentication method Jane should use?

- A. WPA2-PSK
- B. WEP-PSK
- C. CCMP
- D. LEAP

Answer: D

Explanation:

A RADIUS server is a server with a database of user accounts and passwords used as a central authentication database for users requiring network access.

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to reauthenticate frequently; upon each successful authentication, the clients acquire a new WEP key (with the hope that the WEP keys don't live long enough to be cracked). LEAP may be configured to use TKIP instead of dynamic WEP.

QUESTION NO: 862

Ann, a security administrator, wishes to replace their RADIUS authentication with a more secure protocol, which can utilize EAP. Which of the following would BEST fit her objective?

- A. CHAP
- B. SAML
- C. Kerberos
- D. Diameter

Answer: D

Explanation:

Diameter is an authentication, authorization, and accounting protocol that replaces the RADIUS protocol. Diameter Applications extend the base protocol by including new commands and/or attributes, such as those for use of the Extensible Authentication Protocol (EAP).

QUESTION NO: 863

Which of the following is an authentication service that uses UDP as a transport medium?

- A. TACACS+
- B. LDAP
- C. Kerberos
- D. RADIUS

Answer: D

Explanation: RADIUS runs in the application layer and makes use of UDP as transport.

QUESTION NO: 864

Pete, a security auditor, has detected clear text passwords between the RADIUS server and the authenticator. Which of the following is configured in the RADIUS server and what technologies should the authentication protocol be changed to?

- A. PAP, MSCHAPv2
- B. CHAP, PAP
- C. MSCHAPv2, NTLMv2
- D. NTLM, NTLMv2

Answer: A

Explanation:

PAP transmits the username and password to the authentication server in plain text.

MSCHAPv2 is utilized as an authentication option for RADIUS servers that are used for Wi-Fi security using the WPA-Enterprise protocol.

QUESTION NO: 865

RADIUS provides which of the following?

- A. Authentication, Authorization, Availability
- B. Authentication, Authorization, Auditing
- C. Authentication, Accounting, Auditing
- D. Authentication, Authorization, Accounting

Answer: D

Explanation:

The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service. It is for this reason that A, B, and C: are incorrect.

References:

<http://en.wikipedia.org/wiki/RADIUS>

QUESTION NO: 866

Which of the following types of security services are used to support authentication for remote users and devices?

- A. Biometrics
- B. HSM
- C. RADIUS
- D. TACACS

Answer: C

Explanation:

RADIUS authentication phase takes place when a network client connects to a network access server (NAS) and provides authentication credentials. The NAS will then make use of the authentication credentials to issue a RADIUS authentication request to the RADIUS server, which will then exchange RADIUS authentication messages with the NAS.

QUESTION NO: 867

Which of the following relies on the use of shared secrets to protect communication?

- A. RADIUS
- B. Kerberos
- C. PKI
- D. LDAP

Answer: A

Explanation:

Obfuscated passwords are transmitted by the RADIUS protocol via a shared secret and the MD5

hashing algorithm.

QUESTION NO: 868

Ann has taken over as the new head of the IT department. One of her first assignments was to implement AAA in preparation for the company's new telecommuting policy. When she takes inventory of the organizations existing network infrastructure, she makes note that it is a mix of several different vendors. Ann knows she needs a method of secure centralized access to the company's network resources. Which of the following is the BEST service for Ann to implement?

- A. RADIUS
- B. LDAP
- C. SAML
- D. TACACS+

Answer: A

Explanation:

The Remote Authentication Dial In User Service (RADIUS) networking protocol offers centralized Authentication, Authorization, and Accounting (AAA) management for users who make use of a network service.

QUESTION NO: 869

Which of the following is mainly used for remote access into the network?

- A. XTACACS
- B. TACACS+
- C. Kerberos
- D. RADIUS

Answer: D

Explanation:

Most gateways that control access to the network have a RADIUS client component that communicates with the RADIUS server. Therefore, it can be inferred that RADIUS is primarily used for remote access.

QUESTION NO: 870

A system administrator is using a packet sniffer to troubleshoot remote authentication. The administrator detects a device trying to communicate to TCP port 49. Which of the following authentication methods is MOST likely being attempted?

- A. RADIUS
- B. TACACS+
- C. Kerberos
- D. LDAP

Answer: B

Explanation:

TACACS makes use of TCP port 49 by default.

QUESTION NO: 871

Which of the following is an authentication and accounting service that uses TCP for connecting to routers and switches?

- A. DIAMETER
- B. RADIUS
- C. TACACS+
- D. Kerberos

Answer: C

Explanation:

TACACS+ is an authentication, authorization, and accounting (AAA) service that makes use of TCP only.

QUESTION NO: 872

A security administrator has been tasked to ensure access to all network equipment is controlled by a central server such as TACACS+. This type of implementation supports which of the following risk mitigation strategies?

- A. User rights and permissions review
- B. Change management
- C. Data loss prevention
- D. Implement procedures to prevent data theft

Answer: A

Explanation:

Terminal Access Controller Access-Control System (TACACS, and variations like XTACACS and TACACS+) is a client/server-oriented environment, and it operates in a manner similar to RADIUS. Furthermore TACACS+ allows for credential to be accepted from multiple methods. Thus you can perform user rights and permission reviews with TACACS+.

QUESTION NO: 873

Which of the following services are used to support authentication services for several local devices from a central location without the use of tokens?

- A. TACACS+
- B. Smartcards
- C. Biometrics
- D. Kerberos

Answer: A

Explanation:

TACACS allows a client to accept a username and password and send a query to a TACACS authentication server. It would determine whether to accept or deny the authentication request and send a response back. The TIP would then allow access or not based upon the response, not tokens.

QUESTION NO: 874

Which of the following protocols uses TCP instead of UDP and is incompatible with all previous versions?

- A. TACACS
- B. XTACACS
- C. RADIUS
- D. TACACS+

Answer: D

Explanation:

TACACS+ is not compatible with TACACS and XTACACS, and makes use of TCP.

QUESTION NO: 875

Which of the following authentication services should be replaced with a more secure alternative?

- A. RADIUS
- B. TACACS
- C. TACACS+
- D. XTACACS

Answer: B

Explanation:

Terminal Access Controller Access-Control System (TACACS) is less secure than XTACACS, which is a proprietary extension of TACACS, and less secure than TACACS+, which replaced TACACS and XTACACS.

QUESTION NO: 876

In Kerberos, the Ticket Granting Ticket (TGT) is used for which of the following?

- A. Identification
- B. Authorization
- C. Authentication
- D. Multifactor authentication

Answer: C

Explanation:

An authentication ticket, also known as a ticket-granting ticket (TGT), is a small amount of encrypted data that is issued by a server in the Kerberos authentication model to begin the authentication process. When the client receives an authentication ticket, the client sends the ticket back to the server along with additional information verifying the client's identity. The server then issues a service ticket and a session key (which includes a form of password), completing the authorization process for that session.

In the Kerberos model, all tickets are time-stamped and have limited lifetimes. This minimizes the danger that hackers will be able to steal or crack the encrypted data and use it to compromise the system. Ideally, no authentication ticket remains valid for longer than the time an expert hacker would need to crack the encryption. Authentication tickets are session-specific, further improving the security of the system by ensuring that no authentication ticket remains valid after a given session is complete.

QUESTION NO: 877

Which of the following types of authentication packages use credentials in a ticket?

- A. Kerberos
- B. LDAP
- C. TACACS+
- D. RADIUS

Answer: A

Explanation:

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.

The KDC verifies the credentials and then creates a ticket-granting ticket (TGT—a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.

The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.

The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.

The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

QUESTION NO: 878

Which of the following authentication services requires the use of a ticket-granting ticket (TGT) server in order to complete the authentication process?

- A. TACACS+
- B. Secure LDAP
- C. RADIUS
- D. Kerberos

Answer: D

Explanation:

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.

The KDC verifies the credentials and then creates a ticket-granting ticket (TGT—a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.

The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.

The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.

The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

QUESTION NO: 879

A security administrator has installed a new KDC for the corporate environment. Which of the following authentication protocols is the security administrator planning to implement across the organization?

- A. LDAP
- B. RADIUS
- C. Kerberos
- D. XTACACS

Answer: C

Explanation:

The fundamental component of a Kerberos solution is the key distribution centre (KDC), which is responsible for verifying the identity of principles and granting and controlling access within a network environment through the use of secure cryptographic keys and tickets.

QUESTION NO: 880

Jane, a security administrator, has been tasked with explaining authentication services to the company's management team. The company runs an active directory infrastructure. Which of the following solutions BEST relates to the host authentication protocol within the company's environment?

- A. Kerberos
- B. Least privilege
- C. TACACS+
- D. LDAP

Answer: A

Explanation:

Kerberos was accepted by Microsoft as the chosen authentication protocol for Windows 2000 and Active Directory domains that followed.

QUESTION NO: 881

Which of the following types of authentication solutions use tickets to provide access to various resources from a central location?

- A. Biometrics
- B. PKI
- C. ACLs
- D. Kerberos

Answer: D

Explanation:

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.

The KDC verifies the credentials and then creates a ticket-granting ticket (TGT—a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.

The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.

The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.

The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

QUESTION NO: 882

Which of the following authentication services uses a ticket granting system to provide access?

- A. RADIUS
- B. LDAP
- C. TACACS+
- D. Kerberos

Answer: D

Explanation:

The basic process of Kerberos authentication is as follows:

The subject provides logon credentials.

The Kerberos client system encrypts the password and transmits the protected credentials to the KDC.

The KDC verifies the credentials and then creates a ticket-granting ticket (TGT—a hashed form of the subject's password with the addition of a time stamp that indicates a valid lifetime). The TGT is encrypted and sent to the client.

The client receives the TGT. At this point, the subject is an authenticated principle in the Kerberos realm.

The subject requests access to resources on a network server. This causes the client to request a service ticket (ST) from the KDC.

The KDC verifies that the client has a valid TGT and then issues an ST to the client. The ST includes a time stamp that indicates its valid lifetime.

The client receives the ST.

The client sends the ST to the network server that hosts the desired resource.

The network server verifies the ST. If it's verified, it initiates a communication session with the client. From this point forward, Kerberos is no longer involved.

QUESTION NO: 883

An information bank has been established to store contacts, phone numbers and other records.

An application running on UNIX would like to connect to this index server using port 88. Which of the following authentication services would this use this port by default?

- A. Kerberos
- B. TACACS+
- C. Radius
- D. LDAP

Answer: A

Explanation: Kerberos makes use of port 88.

QUESTION NO: 884

Which of the following was based on a previous X.500 specification and allows either unencrypted authentication or encrypted authentication through the use of TLS?

- A. Kerberos
- B. TACACS+
- C. RADIUS
- D. LDAP

Answer: D

Explanation:

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

A common usage of LDAP is to provide a "single sign on" where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet).

LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite.

A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP and UDP port 389, or on port 636 for LDAPS. Global Catalog is available by default on ports 3268, and 3269 for LDAPS. The client then sends an operation request to the server, and the server sends responses in return.

The client may request the following operations:

StartTLS — use the LDAPv3 Transport Layer Security (TLS) extension for a secure connection

QUESTION NO: 885

A system administrator is configuring UNIX accounts to authenticate against an external server. The configuration file asks for the following information DC=ServerName and DC=COM. Which of the following authentication services is being used?

- A. RADIUS
- B. SAML
- C. TACACS+
- D. LDAP

Answer: D

Explanation:

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

An entry can look like this when represented in LDAP Data Interchange Format (LDIF) (LDAP itself is a binary protocol):

```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

"dn" is the distinguished name of the entry; it is neither an attribute nor a part of the entry.

"cn=John Doe" is the entry's RDN (Relative Distinguished Name), and "dc=example,dc=com" is the DN of the parent entry, where "dc" denotes 'Domain Component'. The other lines show the attributes in the entry. Attribute names are typically mnemonic strings, like "cn" for common name, "dc" for domain component, "mail" for e-mail address, and "sn" for surname.

QUESTION NO: 886

Which of the following is an XML based open standard used in the exchange of authentication and authorization information between different parties?

- A. LDAP
- B. SAML
- C. TACACS+
- D. Kerberos

Answer: B

Explanation:

Security Assertion Markup Language (SAML) is an open-standard data format centred on XML. It is used for supporting the exchange of authentication and authorization details between systems, services, and devices.

QUESTION NO: 887

Which of the following is an authentication method that can be secured by using SSL?

- A. RADIUS
- B. LDAP
- C. TACACS+
- D. Kerberos

Answer: B

Explanation:

With secure LDAP (LDAPS), all LDAP communications are encrypted with SSL/TLS

QUESTION NO: 888

A user ID and password together provide which of the following?

- A. Authorization
- B. Auditing
- C. Authentication
- D. Identification

Answer: C

Explanation:

Authentication generally requires one or more of the following:

Something you know: a password, code, PIN, combination, or secret phrase.

Something you have: a smart card, token device, or key.

Something you are: a fingerprint, a retina scan, or voice recognition; often referred to as biometrics, discussed later in this chapter.

Somewhere you are: a physical or logical location.

Something you do: typing rhythm, a secret handshake, or a private knock.

QUESTION NO: 889

The fundamental information security principals include confidentiality, availability and which of the following?

- A.** The ability to secure data against unauthorized disclosure to external sources
- B.** The capacity of a system to resist unauthorized changes to stored information
- C.** The confidence with which a system can attest to the identity of a user
- D.** The characteristic of a system to provide uninterrupted service to authorized users

Answer: B

Explanation: Confidentiality, integrity, and availability, which make up the CIA triad, are the three most important concepts in security. In this instance, the answer describes the Integrity part of the CIA triad.

QUESTION NO: 890

Which of the following is the difference between identification and authentication of a user?

- A.** Identification tells who the user is and authentication tells whether the user is allowed to logon to a system.
- B.** Identification tells who the user is and authentication proves it.
- C.** Identification proves who the user is and authentication is used to keep the users data secure.
- D.** Identification proves who the user is and authentication tells the user what they are allowed to do.

Answer: B

Explanation:

Identification is described as the claiming of an identity, and authentication is described as the act

of verifying or proving the claimed identity.

QUESTION NO: 891

A network administrator has a separate user account with rights to the domain administrator group. However, they cannot remember the password to this account and are not able to login to the server when needed. Which of the following is MOST accurate in describing the type of issue the administrator is experiencing?

- A. Single sign-on
- B. Authorization
- C. Access control
- D. Authentication

Answer: D

Explanation:

Authentication generally requires one or more of the following:

Something you know: a password, code, PIN, combination, or secret phrase.

Something you have: a smart card, token device, or key.

Something you are: a fingerprint, a retina scan, or voice recognition; often referred to as biometrics, discussed later in this chapter.

Somewhere you are: a physical or logical location.

Something you do: typing rhythm, a secret handshake, or a private knock.

QUESTION NO: 892

Ann works at a small company and she is concerned that there is no oversight in the finance department; specifically, that Joe writes, signs and distributes paycheques, as well as other expenditures. Which of the following controls can she implement to address this concern?

- A. Mandatory vacations
- B. Time of day restrictions
- C. Least privilege
- D. Separation of duties

Answer: D

Explanation:

Separation of duties divides administrator or privileged tasks into separate groupings, which in turn, is individually assigned to unique administrators. This helps in fraud prevention, error

reduction, as well as conflict of interest prevention. For example, those who configure security should not be the same people who test security. In this case, Joe should not be allowed to write and sign paycheques.

QUESTION NO: 893

A security administrator implements access controls based on the security classification of the data and need-to-know information. Which of the following BEST describes this level of access control?

- A. Implicit deny
- B. Role-based Access Control
- C. Mandatory Access Controls
- D. Least privilege

Answer: C

Explanation:

Mandatory Access Control allows access to be granted or restricted based on the rules of classification. MAC also includes the use of need to know. Need to know is a security restriction where some objects are restricted unless the subject has a need to know them.

QUESTION NO: 894

Which of the following presents the STRONGEST access control?

- A. MAC
- B. TACACS
- C. DAC
- D. RBAC

Answer: A

Explanation:

A: With Mandatory Access Control (MAC) all access is predefined. This makes it the strongest access control of the options presented in the question.

QUESTION NO: 895

A user reports being unable to access a file on a network share. The security administrator

determines that the file is marked as confidential and that the user does not have the appropriate access level for that file. Which of the following is being implemented?

- A. Mandatory access control
- B. Discretionary access control
- C. Rule based access control
- D. Role based access control

Answer: A

Explanation:

Mandatory Access Control (MAC) allows access to be granted or restricted based on the rules of classification. MAC in corporate business environments involve the following four sensitivity levels

Public

Sensitive

Private

Confidential

MAC assigns subjects a clearance level and assigns objects a sensitivity label. The name of the clearance level must be the same as the name of the sensitivity label assigned to objects or resources. In this case the file is marked confidential, and the user does not have that clearance level and cannot access the file.

QUESTION NO: 896

Which of the following common access control models is commonly used on systems to ensure a "need to know" based on classification levels?

- A. Role Based Access Controls
- B. Mandatory Access Controls
- C. Discretionary Access Controls
- D. Access Control List

Answer: B

Explanation:

Mandatory Access Control allows access to be granted or restricted based on the rules of classification. MAC also includes the use of need to know. Need to know is a security restriction where some objects are restricted unless the subject has a need to know them.

QUESTION NO: 897

Which of the following access controls enforces permissions based on data labeling at specific levels?

- A. Mandatory access control
- B. Separation of duties access control
- C. Discretionary access control
- D. Role based access control

Answer: A

Explanation:

In a MAC environment everything is assigned a classification marker. Subjects are assigned a clearance level and objects are assigned a sensitivity label.

QUESTION NO: 898

Joe Has read and write access to his own home directory. Joe and Ann are collaborating on a project, and Joe would like to give Ann write access to one particular file in this home directory. Which of the following types of access control would this reflect?

- A. Role-based access control
- B. Rule-based access control
- C. Mandatory access control
- D. Discretionary access control

Answer: D

Explanation:

Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner.

QUESTION NO: 899

The IT department has setup a share point site to be used on the intranet. Security has established the groups and permissions on the site. No one may modify the permissions and all requests for access are centrally managed by the security team. This is an example of which of the following control types?

- A. Rule based access control
- B. Mandatory access control
- C. User assigned privilege
- D. Discretionary access control

Answer: D

Explanation:

Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner.

QUESTION NO: 900

A security technician is working with the network firewall team to implement access controls at the company's demarc as part of the initiation of configuration management processes. One of the network technicians asks the security technician to explain the access control type found in a firewall. With which of the following should the security technician respond?

- A. Rule based access control
- B. Role based access control
- C. Discretionary access control
- D. Mandatory access control

Answer: A

Explanation:

Rule-based access control is used for network devices, such as firewalls and routers, which filter traffic based on filtering rules.

QUESTION NO: 901

During the information gathering stage of a deploying role-based access control model, which of the following information is MOST likely required?

- A. Conditional rules under which certain systems may be accessed
- B. Matrix of job titles with required access privileges
- C. Clearance levels of all company personnel
- D. Normal hours of business operation

Answer: B

Explanation:

Role-based access control is a model where access to resources is determined by job role rather than by user account.

Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members or staff (or other system users) are

assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's department.

To configure role-based access control, you need a list (or matrix) of job titles (roles) and the access privileges that should be assigned to each role.

QUESTION NO: 902

A company hired Joe, an accountant. The IT administrator will need to create a new account for Joe. The company uses groups for ease of management and administration of user accounts.

Joe will need network access to all directories, folders and files within the accounting department.

Which of the following configurations will meet the requirements?

- A.** Create a user account and assign the user account to the accounting group.
- B.** Create an account with role-based access control for accounting.
- C.** Create a user account with password reset and notify Joe of the account creation.
- D.** Create two accounts: a user account and an account with full network administration rights.

Answer: B

Explanation:

Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role. The IT administrator should, therefore, create an account with role-based access control for accounting for Joe.

QUESTION NO: 903

Users require access to a certain server depending on their job function. Which of the following would be the MOST appropriate strategy for securing the server?

- A.** Common access card
- B.** Role based access control
- C.** Discretionary access control

D. Mandatory access control

Answer: B

Explanation:

Role-based Access Control is basically based on a user's job description. When a user is assigned a specific role in an environment, that user's access to objects is granted based on the required tasks of that role.

QUESTION NO: 904

The company's sales team plans to work late to provide the Chief Executive Officer (CEO) with a special report of sales before the quarter ends. After working for several hours, the team finds they cannot save or print the reports.

Which of the following controls is preventing them from completing their work?

- A. Discretionary access control**
- B. Role-based access control**
- C. Time of Day access control**
- D. Mandatory access control**

Answer: C

Explanation:

Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours when oversight and monitoring can be performed to prevent fraud, abuse, or intrusion. In this case, the sales team is prevented from saving or printing reports after a certain time.

QUESTION NO: 905

Which of the following security concepts can prevent a user from logging on from home during the weekends?

- A. Time of day restrictions**
- B. Multifactor authentication**
- C. Implicit deny**
- D. Common access card**

Answer: A

Explanation:

Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours when oversight and monitoring can be performed to prevent fraud, abuse, or intrusion.

QUESTION NO: 906

A technician is reviewing the logical access control method an organization uses. One of the senior managers requests that the technician prevent staff members from logging on during nonworking days. Which of the following should the technician implement to meet managements request?

- A. Enforce Kerberos
- B. Deploy smart cards
- C. Time of day restrictions
- D. Access control lists

Answer: C

Explanation: Time of day restrictions limit when users can access specific systems based on the time of day or week. It can limit access to sensitive environments to normal business hours.

QUESTION NO: 907

Ann, the security administrator, wishes to implement multifactor security. Which of the following should be implemented in order to compliment password usage and smart cards?

- A. Hard tokens
- B. Fingerprint readers
- C. Swipe badge readers
- D. Passphrases

Answer: B**Explanation:**

A multifactor authentication method uses two or more processes for logon. A twofactor method might use smart cards and biometrics for logon. For obvious reasons, the two or more factors employed should not be from the same category.

QUESTION NO: 908 HOTSPOT

For each of the given items, select the appropriate authentication category from the drop down choices.

Select the appropriate authentication type for the following items:

Item	Response
Fingerprint scan	<input type="text"/>
Hardware token	<input type="text"/>
Smart card	<input type="text"/>
Password	<input type="text"/>
PIN number	<input type="text"/>
Retina Scan	<input type="text"/>

Item	Response
Fingerprint scan	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Hardware token	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Smart card	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Password	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
PIN number	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>
Retina Scan	<div><div></div><div>Biometric authentication One Time Password Multi-factor PAP authentication PAP authentication Biometric authentication</div></div>

Answer:

Item	Response
Fingerprint scan	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Hardware token	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Smart card	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Password	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
PIN number	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Retina Scan	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>

Explanation:

Item	Response
Fingerprint scan	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Hardware token	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Smart card	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Password	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
PIN number	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>
Retina Scan	<div><div></div><div>Biometric authentication</div><div>One Time Password</div><div>Multi-factor</div><div>PAP authentication</div><div>PAP authentication</div><div>Biometric authentication</div></div>

Biometrics refers to a collection of physical attributes of the human body that can be used as

identification or an authentication factor. Fingerprints and retinas are physical attributes of the human body.

Two types of tokens exist, Time-based one-time password (TOTP) tokens and HMAC-based one-time password (HOTP). TOTP tokens generate passwords at fixed time intervals, whereas HOTP tokens generate passwords not based on fixed time intervals but instead based on a non-repeating one-way function, such as a hash or HMAC operation.

Smart cards can have Multi-factor and proximity authentication embedded into it.

PAP allows for two entities to share a password in advance and use the password as the basis of authentication. The same goes for PIN numbers.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 282, 285

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle

http://en.wikipedia.org/wiki/Smart_card#Security

QUESTION NO: 909

A network administrator uses an RFID card to enter the datacenter, a key to open the server rack, and a username and password to logon to a server. These are examples of which of the following?

- A. Multifactor authentication
- B. Single factor authentication
- C. Separation of duties
- D. Identification

Answer: B

Explanation:

Single-factor authentication (SFA) is a process for securing access to a given system by identifying the party requesting access via a single category of credentials. In this case, the network administrator makes use of an RFID card to access the datacenter, a key to access the server rack, and a username and password to access a server.

QUESTION NO: 910

Use of a smart card to authenticate remote servers remains MOST susceptible to which of the following attacks?

- A. Malicious code on the local system
- B. Shoulder surfing
- C. Brute force certificate cracking
- D. Distributed dictionary attacks

Answer: A

Explanation:

Once a user authenticates to a remote server, malicious code on the user's workstation could then infect the server.

QUESTION NO: 911

Employee badges are encoded with a private encryption key and specific personal information.

The encoding is then used to provide access to the network. Which of the following describes this access control type?

- A. Smartcard
- B. Token
- C. Discretionary access control
- D. Mandatory access control

Answer: A

Explanation:

Smart cards are credit-card-sized IDs, badges, or security passes with an embedded integrated circuit chip that can include data regarding the authorized bearer. This data can then be used for identification and/or authentication purposes.

QUESTION NO: 912

A Chief Information Security Officer (CISO) wants to implement two-factor authentication within the company. Which of the following would fulfill the CISO's requirements?

- A. Username and password
- B. Retina scan and fingerprint scan
- C. USB token and PIN
- D. Proximity badge and token

Answer: C

Explanation:

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:

- knowledge factors ("things only the user knows"), such as passwords
- possession factors ("things only the user has"), such as ATM cards
- inherence factors ("things only the user is"), such as biometrics

In this question, a USB token is a possession factor (something the user has) and a PIN is a knowledge factor (something the user knows).

QUESTION NO: 913

A technician wants to implement a dual factor authentication system that will enable the organization to authorize access to sensitive systems on a need-to-know basis. Which of the following should be implemented during the authorization stage?

- A. Biometrics
- B. Mandatory access control
- C. Single sign-on
- D. Role-based access control

Answer: A

Explanation:

This question is asking about "authorization", not authentication.

Mandatory access control (MAC) is a form of access control commonly employed by government and military environments. MAC specifies that access is granted based on a set of rules rather than at the discretion of a user. The rules that govern MAC are hierarchical in nature and are often called sensitivity labels, security domains, or classifications.

MAC can also be deployed in private sector or corporate business environments. Such cases typically involve the following four security domain levels (in order from least sensitive to most sensitive):

Public
Sensitive
Private
Confidential

A MAC environment works by assigning subjects a clearance level and assigning objects a sensitivity label—in other words, everything is assigned a classification marker. Subjects or users

are assigned clearance levels. The name of the clearance level is the same as the name of the sensitivity label assigned to objects or resources. A person (or other subject, such as a program or a computer system) must have the same or greater assigned clearance level as the resources they wish to access. In this manner, access is granted or restricted based on the rules of classification (that is, sensitivity labels and clearance levels).

MAC is named as it is because the access control it imposes on an environment is mandatory. Its assigned classifications and the resulting granting and restriction of access can't be altered by users. Instead, the rules that define the environment and judge the assignment of sensitivity labels and clearance levels control authorization.

MAC isn't a very granularly controlled security environment. An improvement to MAC includes the use of need to know: a security restriction where some objects (resources or data) are restricted unless the subject has a need to know them. The objects that require a specific need to know are assigned a sensitivity label, but they're compartmentalized from the rest of the objects with the same sensitivity label (in the same security domain). The need to know is a rule in and of itself, which states that access is granted only to users who have been assigned work tasks that require access to the cordoned-off object. Even if users have the proper level of clearance, without need to know, they're denied access. Need to know is the MAC equivalent of the principle of least privilege from DAC

QUESTION NO: 914

Which of the following is an example of multifactor authentication?

- A.** Credit card and PIN
- B.** Username and password
- C.** Password and PIN
- D.** Fingerprint and retina scan

Answer: A

Explanation:

A credit card is a memory card that functions a type of two-factor authentication. The card is something you have, and its PIN is something you know. Multifactor authentication requires a user to provide two or more different types of authentication factors to prove their identity.

QUESTION NO: 915

Which of the following protocols provides for mutual authentication of the client and server?

- A. Two-factor authentication
- B. Radius
- C. Secure LDAP
- D. Biometrics

Answer: C

Explanation:

C: The LDAP directory service is based on a client-server model. The function of LDAP is to enable access to an existing directory. Because it is a client-server model it makes provision for mutual authentication between the two parties.

QUESTION NO: 916

A company with a US-based sales force has requested that the VPN system be configured to authenticate the sales team based on their username, password and a client side certificate.

Additionally, the security administrator has restricted the VPN to only allow authentication from the US territory. How many authentication factors are in use by the VPN system?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

Explanation:

Three different types of authentication factors have been used in this question:

Something you know – username and password.

Something you have - client side certificate.

Somewhere you are - authentication to the VPN is only allowed from the U.S. territory.

QUESTION NO: 917

A company requires that a user's credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

- A. Biometrics
- B. Kerberos
- C. Token

D. Two-factor

Answer: D

Explanation: Two-factor authentication is when two different authentication factors are provided for authentication purposes. In this case, “something they know and something they are”.

QUESTION NO: 918

One of the most basic ways to protect the confidentiality of data on a laptop in the event the device is physically stolen is to implement which of the following?

- A.** File level encryption with alphanumeric passwords
- B.** Biometric authentication and cloud storage
- C.** Whole disk encryption with two-factor authentication
- D.** BIOS passwords and two-factor authentication

Answer: C

Explanation: Whole-disk encryption only provides reasonable protection when the system is fully powered off. to make the most of the defensive strength of whole-disk encryption, a long, complex passphrase should be used to unlock the system on bootup. Combining whole-disk encryption with two factor authentication would further increase protection.

QUESTION NO: 919

Speaking a passphrase into a voice print analyzer is an example of which of the following security concepts?

- A.** Two factor authentication
- B.** Identification and authorization
- C.** Single sign-on
- D.** Single factor authentication

Answer: A

Explanation:

Two-factor authentication is when two different authentication factors are provided for authentication purposes.

Speaking (Voice) – something they are.

Passphrase – something they know.

QUESTION NO: 920

Which of the following BEST describes using a smart card and typing in a PIN to gain access to a system?

- A. Biometrics
- B. PKI
- C. Single factor authentication
- D. Multifactor authentication

Answer: D

Explanation:

Multifactor authentication requires a user to provide two or more authentication factors for authentication purposes. In this case, a smart card (something they have) is one and a PIN (something they know) is the second.

QUESTION NO: 921

An organization has introduced token-based authentication to system administrators due to risk of password compromise. The tokens have a set of numbers that automatically change every 30 seconds. Which of the following type of authentication mechanism is this?

- A. TOTP
- B. Smart card
- C. CHAP
- D. HOTP

Answer: A

Explanation:

Time-based one-time password (TOTP) tokens are devices or applications that generate passwords at fixed time intervals. In this case, it's every 30 seconds.

QUESTION NO: 922

A security technician has been asked to recommend an authentication mechanism that will allow users to authenticate using a password that will only be valid for a predefined time interval. Which of the following should the security technician recommend?

- A. CHAP
- B. TOTP

- C. HOTP
- D. PAP

Answer: B

Explanation: Time-based one-time password (TOTP) tokens are devices or applications that generate passwords at fixed time intervals. Therefore, the password will only be valid for a predefined time interval.

QUESTION NO: 923

LDAP and Kerberos are commonly used for which of the following?

- A. To perform queries on a directory service
- B. To store usernames and passwords for Federated Identity
- C. To sign SSL wildcard certificates for subdomains
- D. To utilize single sign-on capabilities

Answer: D

Explanation:

Single sign-on is usually achieved via the Lightweight Directory Access Protocol (LDAP), although Kerberos can also be used.

QUESTION NO: 924

After Ann, a user, logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. Which of the following is being described?

- A. Trusted OS
- B. Mandatory access control
- C. Separation of duties
- D. Single sign-on

Answer: D

Explanation:

Single sign-on means that once a user (or other subject) is authenticated into a realm, re-authentication is not required for access to resources on any realm entity. The question states that when Ann logs into her banking websites she has access to her financial institution mortgage, credit card, and brokerage websites as well. This describes an SSO scenario.

QUESTION NO: 925

A company wants to ensure that all credentials for various systems are saved within a central database so that users only have to login once for access to all systems. Which of the following would accomplish this?

- A. Multi-factor authentication
- B. Smart card access
- C. Same Sign-On
- D. Single Sign-On

Answer: D

Explanation:

Single sign-on means that once a user (or other subject) is authenticated into a realm, re-authentication is not required for access to resources on any realm entity. Single sign-on is able to internally translate and store credentials for the various mechanisms, from the credential used for original authentication.

QUESTION NO: 926

A user attempting to log on to a workstation for the first time is prompted for the following information before being granted access: username, password, and a four-digit security pin that was mailed to him during account registration. This is an example of which of the following?

- A. Dual-factor authentication
- B. Multifactor authentication
- C. Single factor authentication
- D. Biometric authentication

Answer: C

Explanation:

Multi-factor authentication (MFA) is a method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories: knowledge factors ("things only the user knows"), such as passwords
possession factors ("things only the user has"), such as ATM cards
inherence factors ("things only the user is"), such as biometrics

In this question a username, password, and a four-digit security pin knowledge are all knowledge factors (something the user knows). Therefore, this is single-factor authentication.

QUESTION NO: 927

Which of the following allows a network administrator to implement an access control policy based on individual user characteristics and NOT on job function?

- A. Attributes based
- B. Implicit deny
- C. Role based
- D. Rule based

Answer: A

Explanation:

Attribute-based access control allows access rights to be granted to users via policies, which combine attributes together. The policies can make use of any type of attributes, which includes user attributes, resource attributes and environment attributes.

QUESTION NO: 928

Which of the following is best practice to put at the end of an ACL?

- A. Implicit deny
- B. Time of day restrictions
- C. Implicit allow
- D. SNMP string

Answer: A

Explanation:

An implicit deny clause is implied at the end of each ACL. This implies that if you aren't specifically granted access or privileges for a resource, you're denied access by default. The implicit deny clause is set by the system.

QUESTION NO: 929

Users report that they are unable to access network printing services. The security technician checks the router access list and sees that web, email, and secure shell are allowed. Which of the following is blocking network printing?

- A. Port security
- B. Flood guards
- C. Loop protection

D. Implicit deny

Answer: D

Explanation:

Implicit deny says that if you aren't explicitly granted access or privileges for a resource, you're denied access by default. The scenario does not state that network printing is allowed in the router access list, therefore, it must be denied by default.

QUESTION NO: 930 HOTSPOT

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<input type="text"/>
Smart card	<input type="text"/>
Hardware Token	<input type="text"/>
Password	<input type="text"/>
PIN number	<input type="text"/>
Fingerprint scan	<input type="text"/>

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<div><div>▼</div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Smart card	<div><div>▼</div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Hardware Token	<div><div>▼</div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Password	<div><div>▼</div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
PIN number	<div><div>▼</div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Fingerprint scan	<div><div>▼</div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>

Answer:

Authentication Category

Instructions: When you have completed the simulation, Please Select the Done Button to Submit

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Smart card	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Hardware Token	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Password	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
PIN number	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Fingerprint scan	<div><div></div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>

Explanation:

Select the appropriate authentication type for the following items:

Item	Response
Retina scan	<div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Smart card	<div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Hardware Token	<div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Password	<div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
PIN number	<div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>
Fingerprint scan	<div><div>Something you have</div><div>Something you know</div><div>Something you are</div><div>All given authentication categories</div></div>

Something you are includes fingerprints, retina scans, or voice recognition.

Something you have includes smart cards, token devices, or keys.

Something you know includes a passwords, codes, PINs, combinations, or secret phrases.

Somewhere you are includes a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.

Something you do includes your typing rhythm, a secret handshake, or a private knock.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, p. 285

QUESTION NO: 931

In order for Sara, a client, to logon to her desktop computer, she must provide her username, password, and a four digit PIN. Which of the following authentication methods is Sara using?

- A. Three factor
- B. Single factor
- C. Two factor
- D. Four factor

Answer: B

Explanation:

Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know.

QUESTION NO: 932

The security department has implemented a new laptop encryption product in the environment. The product requires one user name and password at the time of boot up and also another password after the operating system has finished loading. This setup is using which of the following authentication types?

- A. Two-factor authentication
- B. Single sign-on
- C. Multifactor authentication
- D. Single factor authentication

Answer: D

Explanation:

Single-factor authentication is when only one authentication factor is used. In this case, Something you know is being used as an authentication factor. Username, password, and PIN form part of Something you know.

QUESTION NO: 933

Which of the following is a measure of biometrics performance which rates the ability of a system to correctly authenticate an authorized user?

- A. Failure to capture
- B. Type II
- C. Mean time to register
- D. Template capacity

Answer: B

Explanation:

Type II, or false acceptance rate (FAR), is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

QUESTION NO: 934

Use of group accounts should be minimized to ensure which of the following?

- A. Password security
- B. Regular auditing
- C. Baseline management
- D. Individual accountability

Answer: D

Explanation:

Holding users accountable for their actions is part of security, and can only be achieved by users having their own user accounts. To adequately provide accountability, the use of shared or group accounts should be discouraged.

QUESTION NO: 935

The system administrator is tasked with changing the administrator password across all 2000 computers in the organization. Which of the following should the system administrator implement to accomplish this task?

- A. A security group
- B. A group policy
- C. Key escrow
- D. Certificate revocation

Answer: B

Explanation:

Group policy is used to manage Windows systems in a Windows network domain environment by means of a Group Policy Object (GPO). GPO's include a number of settings related to credentials, such as password complexity requirements, password history, password length, account lockout settings.

QUESTION NO: 936

A network inventory discovery application requires non-privileged access to all hosts on a network for inventory of installed applications. A service account is created by the network inventory discovery application for accessing all hosts. Which of the following is the MOST efficient method for granting the account non-privileged access to the hosts?

- A. Implement Group Policy to add the account to the users group on the hosts
- B. Add the account to the Domain Administrator group
- C. Add the account to the Users group on the hosts
- D. Implement Group Policy to add the account to the Power Users group on the hosts.

Answer: A

Explanation:

Group Policy is an infrastructure that allows you to implement specific configurations for users and computers. Group Policy settings are contained in Group Policy objects (GPOs), which are linked to the following Active Directory directory service containers: sites, domains, or organizational units (OUs). This means that if the GPO is linked to the domain, all Users groups in the domain will include the service account.

QUESTION NO: 937

A group policy requires users in an organization to use strong passwords that must be changed every 15 days. Joe and Ann were hired 16 days ago. When Joe logs into the network, he is prompted to change his password; when Ann logs into the network, she is not prompted to change

her password. Which of the following BEST explains why Ann is not required to change her password?

- A. Ann's user account has administrator privileges.
- B. Joe's user account was not added to the group policy.
- C. Ann's user account was not added to the group policy.
- D. Joe's user account was inadvertently disabled and must be re-created.

Answer: C

Explanation:

Group policy is used to manage Windows systems in a Windows network domain environment by means of a Group Policy Object (GPO). GPO's include a number of settings related to credentials, which includes password expiration. Because Anne was not prompted to change her password, it could only mean that her user account was not added to the group policy.

QUESTION NO: 938

An auditing team has found that passwords do not meet best business practices. Which of the following will MOST increase the security of the passwords? (Select TWO).

- A. Password Complexity
- B. Password Expiration
- C. Password Age
- D. Password Length
- E. Password History

Answer: A,D

Explanation:

Passwords should have the strength to avoid discovery through attack, but it should also be easy enough for the user to remember. The length and complexity of a password combined are vital factors in defining a password's strength.

QUESTION NO: 939

Which of the following passwords is the LEAST complex?

- A. MyTrain!45
- B. Mytr@in!!
- C. MyTr@in12
- D. MyTr@in#8

Answer: B

Explanation:

Password policies often enforce a minimum of three out of four standard character types, which includes uppercase and lowercase letters, numbers, and symbols. Although this option includes three of the four character types, it does not include numbers, which makes it less complex than the other options.

QUESTION NO: 940

A security administrator wants to check user password complexity. Which of the following is the BEST tool to use?

- A. Password history
- B. Password logging
- C. Password cracker
- D. Password hashing

Answer: C

Explanation:

The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Password-cracking tools compare hashes from potential passwords with the hashes stored in the accounts database. Each potential password is hashed, and that hash value is compared with the accounts database. If a match is found, the password-cracker tool has discovered a password for a user account.

QUESTION NO: 941

When Ann an employee returns to work and logs into her workstation she notices that, several desktop configuration settings have changed. Upon a review of the CCTV logs, it is determined that someone logged into Ann's workstation. Which of the following could have prevented this from happening?

- A. Password complexity policy
- B. User access reviews
- C. Shared account prohibition policy
- D. User assigned permissions policy

Answer: A

Explanation:

The most important countermeasure against password crackers is to use long, complex passwords, which are changed regularly. Since changes were made to Ann's desktop configuration settings while she was not at work, means that her password was compromised.

QUESTION NO: 942

After a recent internal audit, the security administrator was tasked to ensure that all credentials must be changed within 90 days, cannot be repeated, and cannot contain any dictionary words or patterns. All credentials will remain enabled regardless of the number of attempts made. Which of the following types of user account options were enforced? (Select TWO).

- A. Recovery
- B. User assigned privileges
- C. Lockout
- D. Disablement
- E. Group based privileges
- F. Password expiration
- G. Password complexity

Answer: F,G

Explanation:

Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character type complexity, the more resistant it is to password-cracking techniques. In most cases, passwords are set to expire every 90 days.

QUESTION NO: 943

An internal auditing team would like to strengthen the password policy to support special characters. Which of the following types of password controls would achieve this goal?

- A. Add reverse encryption
- B. Password complexity
- C. Increase password length
- D. Allow single sign on

Answer: B

Explanation:

Generally, the minimum password length is considered to be 8 upper and lowercase characters. The use of at least one non-alpha character like punctuation, special characters, or numbers,

combined with the password length produces strong passwords. Strong passwords are produced by the combination of a password's length and complexity.

QUESTION NO: 944

The systems administrator notices that many employees are using passwords that can be easily guessed or are susceptible to brute force attacks. Which of the following would BEST mitigate this risk?

- A. Enforce password rules requiring complexity.
- B. Shorten the maximum life of account passwords.
- C. Increase the minimum password length.
- D. Enforce account lockout policies.

Answer: A

Explanation:

Password complexity often requires the use of a minimum of three out of four standard character types for a password. The more characters in a password that includes some character complexity, the more resistant it is to brute force attacks.

QUESTION NO: 945

Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

- A. A recent security breach in which passwords were cracked.
- B. Implementation of configuration management processes.
- C. Enforcement of password complexity requirements.
- D. Implementation of account lockout procedures.

Answer: A

Explanation:

A password only needs to be changed if it doesn't meet the compliance requirements of the company's password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion.

QUESTION NO: 946

A security administrator is concerned about the strength of user's passwords. The company does not want to implement a password complexity policy. Which of the following can the security Administrator implement to mitigate the risk of an online password attack against users with weak passwords?

- A. Increase the password length requirements
- B. Increase the password history
- C. Shorten the password expiration period
- D. Decrease the account lockout time

Answer: C

Explanation:

Reducing the password expiration period will require passwords to be changed at the end of that period. A password needs to be changed if it doesn't meet the compliance requirements of the company's password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion. This will give online password attackers less time to crack the weak passwords.

QUESTION NO: 947

Which of the following should be done before resetting a user's password due to expiration?

- A. Verify the user's domain membership.
- B. Verify the user's identity.
- C. Advise the user of new policies.
- D. Verify the proper group membership.

Answer: B

Explanation:

When resetting a password, users have to establish their identity by answering a series of personal questions, using a hardware authentication token, or responding to a password notification e-mail. Users can then either specify a new, unlocked password, or ask that a randomly generated one be provided. This can be done from their workstation login prompt, or through a telephone call.

QUESTION NO: 948

The IT department has setup a website with a series of questions to allow end users to reset their own accounts. Which of the following account management practices does this help?

- A. Account Disablements
- B. Password Expiration
- C. Password Complexity
- D. Password Recovery

Answer: D

Explanation:

People tend to forget their own passwords and because a user's password is not stored on the operating system, only a hash value is kept and most operating systems allow the administrator to change the value meaning that the password can then be recovered. If you allow end users to reset their own accounts then the password recovery process is helped along.

QUESTION NO: 949

An insurance company requires an account recovery process so that information created by an employee can be accessed after that employee is no longer with the firm. Which of the following is the BEST approach to implement this process?

- A. Employee is required to share their password with authorized staff prior to leaving the firm
- B. Passwords are stored in a reversible form so that they can be recovered when needed
- C. Authorized employees have the ability to reset passwords so that the data is accessible
- D. All employee data is exported and imported by the employee prior to them leaving the firm

Answer: C

Explanation:

Since a user's password isn't stored on most operating systems (only a hash value is kept), most operating systems allow the administrator (or authorized person in this case) to change the value then the information/files/documents can be accessed. This is the safest way of recovery by an authorized person and is not dependent on those who leave the firm.

QUESTION NO: 950

A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access.

Which of the following is the BEST approach to implement this process?

- A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.

- B.** Require the customer to physically come into the company's main office so that the customer can be authenticated prior to their password being reset.
- C.** Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.
- D.** Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login.

Answer: D

Explanation:

People tend to forget their passwords, thus you should have a password recovery system for them that will not increase risk exposure. Setting a temporary password will restrict the time that the password is valid and thus decrease risk; and in addition forcing the customer to change it upon first login will make the password more secure for the customer.

QUESTION NO: 951

A user has forgotten their account password. Which of the following is the BEST recovery strategy?

- A.** Upgrade the authentication system to use biometrics instead.
- B.** Temporarily disable password complexity requirements.
- C.** Set a temporary password that expires upon first use.
- D.** Retrieve the user password from the credentials database.

Answer: C

Explanation:

Since a user's password isn't stored on most operating systems (only a hash value is kept), most operating systems allow the administrator to change the value for a user who has forgotten theirs. This new value allows the user to log in and then immediately change it to another value that they can (ideally) remember. Also setting a temporary password to expire upon first use will not allow a hacker the opportunity or time to use it.

QUESTION NO: 952

Which of the following is a BEST practice when dealing with user accounts that will only need to be active for a limited time period?

- A.** When creating the account, set the account to not remember password history.
- B.** When creating the account, set an expiration date on the account.
- C.** When creating the account, set a password expiration date on the account.

D. When creating the account, set the account to have time of day restrictions.

Answer: B

Explanation:

Disablement is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

QUESTION NO: 953

ABC company has a lot of contractors working for them. The provisioning team does not always get notified that a contractor has left the company. Which of the following policies would prevent contractors from having access to systems in the event a contractor has left?

- A. Annual account review
- B. Account expiration policy
- C. Account lockout policy
- D. Account disablement

Answer: B

Explanation:

Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

QUESTION NO: 954

Which of the following controls mitigates the risk of Matt, an attacker, gaining access to a company network by using a former employee's credential?

- A. Account expiration
- B. Password complexity
- C. Account lockout
- D. Dual factor authentication

Answer: A

Explanation:

Account expiration is a secure feature to employ on user accounts for temporary workers, interns, or consultants. It automatically disables a user account or causes the account to expire at a specific time and on a specific day.

QUESTION NO: 955

Which of the following security benefits would be gained by disabling a terminated user account rather than deleting it?

- A. Retention of user keys
- B. Increased logging on access attempts
- C. Retention of user directories and files
- D. Access to quarantined files

Answer: A

Explanation:

Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account and that the user keys for that account are retained which would not be the case if the account was deleted from the system.

QUESTION NO: 956

During an audit, the security administrator discovers that there are several users that are no longer employed with the company but still have active user accounts. Which of the following should be performed?

- A. Account recovery
- B. Account disablement
- C. Account lockouts
- D. Account expiration

Answer: B

Explanation:

Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account.

QUESTION NO: 957

A hacker has discovered a simple way to disrupt business for the day in a small company which relies on staff working remotely. In a matter of minutes the hacker was able to deny remotely working staff access to company systems with a script. Which of the following security controls is the hacker exploiting?

- A. DoS
- B. Account lockout
- C. Password recovery
- D. Password complexity

Answer: B

Explanation:

B: Account lockout automatically disables an account due to repeated failed log on attempts. The hacker must have executed a script to repeatedly try logging on to the remote accounts, forcing the account lockout policy to activate.

QUESTION NO: 958

Account lockout is a mitigation strategy used by Jane, the administrator, to combat which of the following attacks? (Select TWO).

- A. Spoofing
- B. Man-in-the-middle
- C. Dictionary
- D. Brute force
- E. Privilege escalation

Answer: C,D

Explanation:

Account lockout is a useful method for slowing down online password-guessing attacks. A dictionary attack performs password guessing by making use of a pre-existing list of likely passwords. A brute-force attack is intended to try every possible valid combination of characters to create possible passwords in the attempt to discover the specific passwords used by user accounts.

QUESTION NO: 959

A recent audit has discovered that at the time of password expiration clients are able to recycle the previous credentials for authentication. Which of the following controls should be used together to prevent this from occurring? (Select TWO).

- A. Password age
- B. Password hashing
- C. Password complexity
- D. Password history
- E. Password length

Answer: A,D

Explanation:

D: Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

A: When a user is forced to change his password due to a maximum password age period expiring, he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

QUESTION NO: 960

A password history value of three means which of the following?

- A. Three different passwords are used before one can be reused.
- B. A password cannot be reused once changed for three years.
- C. After three hours a password must be re-entered to continue.
- D. The server stores passwords in the database for three days.

Answer: A

Explanation:

Password History defines the number of unique new passwords a user must use before an old password can be reused.

QUESTION NO: 961

An administrator discovers that many users have used their same passwords for years even though the network requires that the passwords be changed every six weeks. Which of the following, when used together, would BEST prevent users from reusing their existing password? (Select TWO).

- A. Length of password
- B. Password history
- C. Minimum password age
- D. Password expiration
- E. Password complexity
- F. Non-dictionary words

Answer: B,C

Explanation:

In this question, users are forced to change their passwords every six weeks. However, they are able to change their password and enter the same password as the new password.

Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

When a user is forced to change his password due to a maximum password age period expiring, (the question states that the network requires that the passwords be changed every six weeks) he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

QUESTION NO: 962

A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

- A. Assign users passwords based upon job role.
- B. Enforce a minimum password age policy.
- C. Prevent users from choosing their own passwords.
- D. Increase the password expiration time frame.

Answer: B

Explanation:

A minimum password age policy defines the period that a password must be used for before it can be changed.

QUESTION NO: 963

Which of the following is an important implementation consideration when deploying a wireless network that uses a shared password?

- A. Authentication server
- B. Server certificate
- C. Key length
- D. EAP method

Answer: C

Explanation:

Key length is the main issue of concern since the wireless network uses a shared password. With risks of shared passwords makes the length of the password a crucial factor to risk mitigation.

QUESTION NO: 964

A security administrator is reviewing the below output from a password auditing tool:

P@ss.

@pW1.

S3cU4

Which of the following additional policies should be implemented based on the tool's output?

- A. Password age
- B. Password history
- C. Password length
- D. Password complexity

Answer: C

Explanation:

The output shows that all the passwords are either 4 or 5 characters long. This is way too short, 8 characters are shown to be the minimum for password length.

QUESTION NO: 965

Several employee accounts appear to have been cracked by an attacker. Which of the following

should the security administrator implement to mitigate password cracking attacks? (Select TWO).

- A. Increase password complexity
- B. Deploy an IDS to capture suspicious logins
- C. Implement password history
- D. Implement monitoring of logins
- E. Implement password expiration
- F. Increase password length

Answer: A,F

Explanation:

The more difficult a password is the more difficult it is to be cracked by an attacker. By increasing the password complexity you make it more difficult.

Passwords that are too short can easily be cracked. The more characters used in a password, combined with the increased complexity will mitigate password cracking attacks.

QUESTION NO: 966

Human Resources suspect an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?

- A. Shared accounts should be prohibited.
- B. Account lockout should be enabled
- C. Privileges should be assigned to groups rather than individuals
- D. Time of day restrictions should be in use

Answer: A

Explanation:

Since distinguishing between the actions of one person and another isn't possible if they both use a shared account, shared accounts should not be allowed. If shared accounts are being used, the administrator will find the account, but have more than one suspect. To nullify this occurrence, Shared accounts should be prohibited.

QUESTION NO: 967

A network administrator is configuring access control for the sales department which has high employee turnover. Which of the following is BEST suited when assigning user rights to individuals in the sales department?

- A. Time of day restrictions
- B. Group based privileges
- C. User assigned privileges
- D. Domain admin restrictions

Answer: B

Explanation:

The question states that the sales department has a high employee turnover. You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). Then when a new employee starts, you simply add the new user account to the appropriate groups. The user then inherits all the permissions assigned to the groups.

QUESTION NO: 968

A new network administrator is setting up a new file server for the company. Which of the following would be the BEST way to manage folder security?

- A. Assign users manually and perform regular user access reviews
- B. Allow read only access to all folders and require users to request permission
- C. Assign data owners to each folder and allow them to add individual users to each folder
- D. Create security groups for each folder and assign appropriate users to each group

Answer: D

Explanation:

Creating a security group for each folder and assigning necessary users to each group would only allow users belonging to the folder's security group access to the folder. It will make assigning folder privileges much easier, while also being more secure.

QUESTION NO: 969

A new intern was assigned to the system engineering department, which consists of the system architect and system software developer's teams. These two teams have separate privileges. The intern requires privileges to view the system architectural drawings and comment on some software development projects. Which of the following methods should the system administrator implement?

- A. Group based privileges
- B. Generic account prohibition
- C. User access review

D. Credential management**Answer: A****Explanation:**

You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). By assigning the intern's user account to both groups, the intern will inherit the permissions assigned to those groups.

QUESTION NO: 970

A system administrator needs to ensure that certain departments have more restrictive controls to their shared folders than other departments. Which of the following security controls would be implemented to restrict those departments?

- A.** User assigned privileges
- B.** Password disablement
- C.** Multiple account creation
- D.** Group based privileges

Answer: D**Explanation:**

Group-based privileges assign privileges or access to a resource to all members of a group. Group-based access control grants every member of the group the same level of access to a specific object.

QUESTION NO: 971

Which of the following practices reduces the management burden of access management?

- A.** Password complexity policies
- B.** User account audit
- C.** Log analysis and review
- D.** Group based privileges

Answer: D

Explanation: Granting permissions to all members of a group is quicker than individually assigning them to each user. This means an administrator will spend less time on assigning permissions to users who require the same access privileges.

QUESTION NO: 972

A supervisor in the human resources department has been given additional job duties in the accounting department. Part of their new duties will be to check the daily balance sheet calculations on spreadsheets that are restricted to the accounting group. In which of the following ways should the account be handled?

- A.** The supervisor should be allowed to have access to the spreadsheet files, and their membership in the human resources group should be terminated.
- B.** The supervisor should be removed from the human resources group and added to the accounting group.
- C.** The supervisor should be added to the accounting group while maintaining their membership in the human resources group.
- D.** The supervisor should only maintain membership in the human resources group.

Answer: C

Explanation:

You can assign permissions to access resources either to a user or a group. The most efficient way is to assign permissions to a group (group based privileges). By assigning the human resources supervisor's user account to the group means the supervisor will inherit the permissions of that group, and allow him to carry out the new duties. Because the new duties are being added to his normal duties, maintaining membership in the human resources group will allow the supervisor to continue performing his normal duties.

QUESTION NO: 973

A security analyst implemented group-based privileges within the company active directory. Which of the following account management techniques should be undertaken regularly to ensure least privilege principles?

- A.** Leverage role-based access controls.
- B.** Perform user group clean-up.
- C.** Verify smart card access controls.
- D.** Verify SHA-256 for password hashes.

Answer: B

Explanation: Active Directory (AD) has no built-in clean-up feature. This can result in obsolete user, group and computer objects accumulating over time and placing security and compliance objectives in jeopardy. You would therefore need to regularly clean-up these settings.

QUESTION NO: 974

Privilege creep among long-term employees can be mitigated by which of the following procedures?

- A. User permission reviews
- B. Mandatory vacations
- C. Separation of duties
- D. Job function rotation

Answer: A

Explanation:

Privilege creep is the steady build-up of access rights beyond what a user requires to perform his/her task. Privilege creep can be decreased by conducting sporadic access rights reviews, which will confirm each user's need to access specific roles and rights in an effort to find and rescind excess privileges.

QUESTION NO: 975

A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid this scenario? (Select TWO).

- A. Automatically disable accounts that have not been utilized for at least 10 days.
- B. Utilize automated provisioning and de-provisioning processes where possible.
- C. Request that employees provide a list of systems that they have access to prior to leaving the firm.
- D. Perform regular user account review / revalidation process.
- E. Implement a process where new account creations require management approval.

Answer: B,D

Explanation:

Provisioning and de-provisioning processes can occur manually or automatically. Since the manual processes are so time consuming, the automated option should be used as it is more efficient. Revalidating user accounts would determine which users are no longer active.

QUESTION NO: 976

In order for network monitoring to work properly, you need a PC and a network card running in what mode?

- A. Launch
- B. Exposed
- C. Promiscuous
- D. Sweep

Answer: C

Explanation:

Promiscuous mode allows the network card to look at any packet that it sees on the network. This even includes packets that are not addressed to that network card.

QUESTION NO: 977

Which of the following techniques enables a highly secured organization to assess security weaknesses in real time?

- A. Access control lists
- B. Continuous monitoring
- C. Video surveillance
- D. Baseline reporting

Answer: B

Explanation:

Continuous monitoring point toward the never-ending review of what resources a user actually accesses, which is critical for preventing insider threats. Because the process is never-ending, assessments happen in real time.

QUESTION NO: 978

A customer has provided an email address and password to a website as part of the login process. Which of the following BEST describes the email address?

- A. Identification
- B. Authorization
- C. Access control
- D. Authentication

Answer: A

Explanation:

Identification is defined as the claiming of an identity and only has to take place once per authentication or access process. A login process typically consists of an identification such as a

username or email address and an authentication which proves you are who you say you are.

QUESTION NO: 979

A company has 5 users. Users 1, 2 and 3 need access to payroll and users 3, 4 and 5 need access to sales. Which of the following should be implemented to give the appropriate access while enforcing least privilege?

- A.** Assign individual permissions to users 1 and 2 for payroll. Assign individual permissions to users 4 and 5 for sales. Make user 3 an administrator.
- B.** Make all users administrators and then restrict users 1 and 2 from sales. Then restrict users 4 and 5 from payroll.
- C.** Create two additional generic accounts, one for payroll and one for sales that users utilize.
- D.** Create a sales group with users 3, 4 and 5. Create a payroll group with users 1, 2 and 3.

Answer: D

Explanation:

Assigning permissions to a group requires less effort than assigning permissions to individual users. When you have groups configured with the appropriate permissions, you can grant the permissions to individual users by adding the users to the groups. Users can be members of multiple groups and therefore have multiple sets of permissions assigned to them. In this answer, user 3 is a member of both groups which grants the user permission to both Sales and Payroll.

QUESTION NO: 980

An administrator implements SELinux on a production web server. After implementing this, the web server no longer serves up files from users' home directories. To rectify this, the administrator creates a new policy as the root user. This is an example of which of the following? (Select TWO).

- A.** Enforcing SELinux in the OS kernel is role-based access control
- B.** Enforcing SELinux in the OS kernel is rule-based access control
- C.** The policy added by the root user is mandatory access control
- D.** Enforcing SELinux in the OS kernel is mandatory access control
- E.** The policy added by the root user is role-based access control
- F.** The policy added by the root user is rule-based access control

Answer: D,F

Explanation:

Enforcing SELinux in the OS kernel is mandatory access control. SELinux is Security Enhanced Linux which is a locked down version of the OS kernel.

Mandatory Access Control (MAC) is a relatively inflexible method for how information access is permitted. In a MAC environment, all access capabilities are predefined. Users can't share information unless their rights to share it are established by administrators. Consequently, administrators must make any changes that need to be made to such rights. This process enforces a rigid model of security. However, it is also considered the most secure security model.

The policy added by the root user is rule-based access control. The administrator has defined a policy that states that users folders should be served by the web server.

Rule-Based Access Control (RBAC) uses the settings in preconfigured security policies to make all decisions.

QUESTION NO: 981

A security administrator has deployed all laptops with Self Encrypting Drives (SED) and enforces key encryption. Which of the following represents the greatest threat to maintaining data confidentiality with these devices?

- A.** Full data access can be obtained by connecting the drive to a SATA or USB adapter bypassing the SED hardware.
- B.** A malicious employee can gain the SED encryption keys through software extraction allowing access to other laptops.
- C.** If the laptop does not use a Secure Boot BIOS, the SED hardware is not enabled allowing full data access.
- D.** Laptops that are placed in a sleep mode allow full data access when powered back on.

Answer: D

Explanation:

Hardware-based encryption when built into the drive is transparent to the user. The drive except for bootup authentication operates just like any drive with no degradation in performance. When the computer is started up, the user is prompted to enter a password to allow the system to boot and allow access to the encrypted drive.

When a laptop is placed into sleep mode (also known as standby mode), the computer is placed into a low power mode. In sleep mode, the computer is not fully shut down. The screen is turned off, the hard disks are turned off and the CPU is throttled down to its lowest power state. However, the computer state is maintained in memory (RAM).

Most computers can be 'woken' from sleep mode by pressing any key on the keyboard or pressing the power button. The computer can be configured to require a password on wake up, but if a password is not required, the computer will wake up and be logged in as it was at the time of going into sleep mode. This would enable full access to the data stored on the disks.

QUESTION NO: 982

A recent review of accounts on various systems has found that after employees' passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Select TWO).

- A. Reverse encryption
- B. Minimum password age
- C. Password complexity
- D. Account lockouts
- E. Password history
- F. Password expiration

Answer: B,E

Explanation:

E: Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords.

B: When a user is forced to change his password due to a maximum password age period expiring, he could change his password to a previously used password. Or if a password history value of 5 is configured, the user could change his password six times to cycle back round to his original password. This is where the minimum password age comes in. This is the period that a password must be used for. For example, a minimum password age of 30 would determine that when a user changes his password, he must continue to use the same password for at least 30 days.

QUESTION NO: 983

An organizations' security policy requires that users change passwords every 30 days. After a security audit, it was determined that users were recycling previously used passwords. Which of the following password enforcement policies would have mitigated this issue?

- A. Password history
- B. Password complexity
- C. Password length
- D. Password expiration

Answer: A

Explanation:

Password history determines the number of previous passwords that cannot be used when a user changes his password. For example, a password history value of 5 would disallow a user from changing his password to any of his previous 5 passwords. However, without a minimum

password age setting, the user could change his password six times and cycle back to his original password.

QUESTION NO: 984

A security administrator must implement a system that will support and enforce the following file system access control model:

FILE NAMESECURITY LABEL

Employees.docConfidential

Salary.xlsConfidential

OfficePhones.xlsUnclassified

PersonalPhones.xlsRestricted

Which of the following should the security administrator implement?

- A. White and black listing
- B. SCADA system
- C. Trusted OS
- D. Version control

Answer: C

Explanation:

A trusted operating system (TOS) is any operating system that meets the government's requirements for security. Trusted OS uses a form of Mandatory access control called Multi-Level Security.

The Mandatory access control (MAC) is a form of access control commonly employed by government and military environments. MAC specifies that access is granted based on a set of rules rather than at the discretion of a user. The rules that govern MAC are hierarchical in nature and are often called sensitivity labels, security domains, or classifications.

MLS is an implementation of MAC that focuses on confidentiality. A Multi-Level Security operating system is able to enforce the separation of multiple classifications of information as well as manage multiple users with varying levels of information clearance. The military and intelligence community must handle and process various hierarchical levels of classified information. At the high-end there is Top Secret, followed in turn by Secret, Confidential, and Unclassified:

QUESTION NO: 985

Which of the following is the BEST reason for placing a password lock on a mobile device?

- A. Prevents an unauthorized user from accessing owner's data
- B. Enables remote wipe capabilities
- C. Stops an unauthorized user from using the device again
- D. Prevents an unauthorized user from making phone calls

Answer: A

Explanation:

A password lock on a mobile device is used to prevent an unauthorized user from accessing owner's data. When a device is turned off either by being manually switched off or by automatically turning off after a timeout, the device will automatically lock. When you turn the device on, you are prompted to enter a password or numeric code to gain access to the device.

QUESTION NO: 986

Ann is the data owner of financial records for a company. She has requested that she have the ability to assign read and write privileges to her folders. The network administrator is tasked with setting up the initial access control system and handing Ann's administrative capabilities. Which of the following systems should be deployed?

- A. Role-based
- B. Mandatory
- C. Discretionary
- D. Rule-based

Answer: C

Explanation:

In a Discretionary Access Control (DAC) model, network users have some flexibility regarding how information is accessed. This model allows users to share information dynamically with other users.

Discretionary access control (DAC) allows access to be granted or restricted by an object's owner based on user identity and on the discretion of the object owner.

In this question, Ann has requested that she have the ability to assign read and write privileges to her folders. Read and write access to Ann's files will be granted by Ann at her discretion.

Therefore, this is an example of Discretionary Access Control.

QUESTION NO: 987

Ann was reviewing her company's event logs and observed several instances of GUEST accessing the company print server, file server, and archive database. As she continued to investigate, Ann noticed that it seemed to happen at random intervals throughout the day, but mostly after the weekly automated patching and often logging in at the same time. Which of the following would BEST mitigate this issue?

- A. Enabling time of day restrictions
- B. Disabling unnecessary services
- C. Disabling unnecessary accounts
- D. Rogue machine detection

Answer: C

Explanation:

User account control is a very important part of operating system hardening. It is important that only active accounts be operational and that they be properly managed. This means disabling unnecessary accounts.

Enabled accounts that are not needed on a system provide a door through which attackers can gain access. You should disable all accounts that are not needed immediately—on servers and workstations alike. Here are some types of accounts that you should disable:

Employees Who Have Left the Company: Be sure to disable immediately accounts for any employee who has left the company. This should be done the minute employment is terminated.

Temporary Employees: It is not uncommon to create short-term accounts for brief periods of time for access by temporary employees. These also need to be disabled the moment they are no longer needed.

Default Guest Accounts: In many operating systems, a guest account is created during installation and intended for use by those needing only limited access and lacking their own account on the system. This account presents a door into the system that should not be there, and all who have worked with the operating system knows of its existence, thus making it a likely target for attackers.

QUESTION NO: 988

Ann is a member of the Sales group. She needs to collaborate with Joe, a member of the IT group, to edit a file. Currently, the file has the following permissions:

Ann:read/write

Sales Group:read

IT Group:no access

If a discretionary access control list is in place for the files owned by Ann, which of the following would be the BEST way to share the file with Joe?

- A. Add Joe to the Sales group.
- B. Have the system administrator give Joe full access to the file.
- C. Give Joe the appropriate access to the file directly.
- D. Remove Joe from the IT group and add him to the Sales group.

Answer: C

Explanation:

Joe needs access to only one file. He also needs to 'edit' that file. Editing a file requires Read and Write access to the file. The best way to provide Joe with the minimum required permissions to edit the file would be to give Joe the appropriate access to the file directly.

QUESTION NO: 989

A network administrator, Joe, arrives at his new job to find that none of the users have changed their network passwords since they were initially hired. Joe wants to have everyone change their passwords immediately. Which of the following policies should be enforced to initiate a password change?

- A. Password expiration
- B. Password reuse
- C. Password recovery
- D. Password disablement

Answer: A

Explanation:

The Maximum password age policy setting determines the number of days that a password can be used before the system requires the user to change it. The password expiration setting determines that a user will not be able to log into a system without changing their password after the maximum password age has been reached.

QUESTION NO: 990

Ann, a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?

- A. Deploy a HIDS suite on the users' computers to prevent application installation.
- B. Maintain the baseline posture at the highest OS patch level.
- C. Enable the pop-up blockers on the users' browsers to prevent malware.
- D. Create an approved application list and block anything not on it.

Answer: D

Explanation:

You can use Software Restriction Policy or its successor AppLocker to prevent unauthorized applications from running or being installed on computers.

Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run.

Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.

You can use AppLocker as part of your overall security strategy for the following scenarios:

Help prevent malicious software (malware) and unsupported applications from affecting computers in your environment.

Prevent users from installing and using unauthorized applications.

Implement application control policy to satisfy portions of your security policy or compliance requirements in your organization.

QUESTION NO: 991

Which of the following should be used to authenticate and log connections from wireless users connecting with EAP-TLS?

- A. Kerberos
- B. LDAP
- C. SAML
- D. RADIUS

Answer: D

Explanation:

EAP-TLS, defined in RFC 2716, is an IETF open standard, and is well-supported among wireless vendors. It offers a good deal of security, since TLS is considered the successor of the SSL standard. It uses PKI to secure communication to the RADIUS authentication server.

Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

QUESTION NO: 992

Ann has recently transferred from the payroll department to engineering. While browsing file shares, Ann notices she can access the payroll status and pay rates of her new coworkers. Which of the following could prevent this scenario from occurring?

- A. Credential management
- B. Continuous monitoring
- C. Separation of duties
- D. User access reviews

Answer: D

Explanation:

In addition to assigning user access properly, it is important to review that access periodically. Access review is a process to determine whether a user's access level is still appropriate. People's roles within an organization can change over time. It is important to review user accounts periodically and determine if they still require the access they currently have. An example of such a scenario would be a network administrator who was responsible for the domain controller but then moved over to administer the remote access servers. The administrator's access to the domain controller should now be terminated. This concept of access review is closely related to the concept of least privileges. It is important that users do not have "leftover" privileges from previous job roles.

QUESTION NO: 993

An organization's security policy states that users must authenticate using something you do. Which of the following would meet the objectives of the security policy?

- A. Fingerprint analysis
- B. Signature analysis
- C. Swipe a badge
- D. Password

Answer: B

Explanation:

Authentication systems or methods are based on one or more of these five factors:

Something you know, such as a password or PIN

Something you have, such as a smart card, token, or identification device

Something you are, such as your fingerprints or retinal pattern (often called biometrics)

Something you do, such as an action you must take to complete authentication

Somewhere you are (this is based on geolocation)

Writing your signature on a document is 'something you do'. Someone can then analyze the signature to see if it matches one stored on record.

QUESTION NO: 994

Which of the following protocols is MOST likely to be leveraged by users who need additional information about another user?

- A. LDAP**
- B. RADIUS**
- C. Kerberos**
- D. TACACS+**

Answer: A

Explanation:

A 'directory' contains information about users.

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories.

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

QUESTION NO: 995

The security manager wants to unify the storage of credential, phone numbers, office numbers, and address information into one system. Which of the following is a system that will support the requirement on its own?

- A. LDAP**

- B. SAML
- C. TACACS
- D. RADIUS

Answer: A

Explanation:

A 'directory' contains information about users.

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories.

The Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

QUESTION NO: 996

Joe, a network administrator, is able to manage the backup software console by using his network login credentials. Which of the following authentication services is the MOST likely using?

- A. SAML
- B. LDAP
- C. iSCSI
- D. Two-factor authentication

Answer: B

Explanation:

Joe is able to manage the backup system by logging into the network. This is an example of Single Sign-on.

A common usage of LDAP is to provide a "single sign on" where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet).

The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network. Directory services play an important role in developing intranet

and Internet applications by allowing the sharing of information about users, systems, networks, services, and applications throughout the network. As examples, directory services may provide any organized set of records, often with a hierarchical structure, such as a corporate email directory. Similarly, a telephone directory is a list of subscribers with an address and a phone number.

QUESTION NO: 997

An organization is implementing a password management application which requires that all local administrator passwords be stored and automatically managed. Auditors will be responsible for monitoring activities in the application by reviewing the logs. Which of the following security controls is the BEST option to prevent auditors from accessing or modifying passwords in the application?

- A. Time of day restrictions
- B. Create user accounts for the auditors and assign read-only access
- C. Mandatory access control
- D. Role-based access with read-only

Answer: D

Explanation:

Auditors (employees performing the auditor role) will have access application by reviewing the logs. We can therefore assign access based on employee role. This is an example of Role-based access control (RBAC).

To prevent the auditors from modifying passwords in the application, we need to ensure that they do not have write access. Therefore, you should assign only read access.

Role-Based Access Control (RBAC) models approach the problem of access control based on established roles in an organization. RBAC models implement access by job function or by responsibility. Each employee has one or more roles that allow access to specific information. If a person moves from one role to another, the access for the previous role will no longer be available.

Instead of thinking "Denise needs to be able to edit files," RBAC uses the logic "Editors need to be able to edit files" and "Denise is a member of the Editors group." This model is always good for use in an environment in which there is high employee turnover.

QUESTION NO: 998

A security administrator is tackling issues related to authenticating users at a remote site. There

have been a large number of security incidents that resulted from either tailgating or impersonation of authorized users with valid credentials. The security administrator has been told to implement multifactor authentication in order to control facility access. To secure access to the remote facility, which of the following could be implemented without increasing the amount of space required at the entrance?

- A. MOTD challenge and PIN pad
- B. Retina scanner and fingerprint reader
- C. Voice recognition and one-time PIN token
- D. One-time PIN token and proximity reader

Answer: C

Explanation:

Authentication systems or methods are based on one or more of these five factors:

Something you know, such as a password or PIN

Something you have, such as a smart card, token, or identification device

Something you are, such as your fingerprints or retinal pattern (often called biometrics)

Something you do, such as an action you must take to complete authentication

Somewhere you are (this is based on geolocation)

Multifactor authentication is authentication that uses two or more of the authentication factors listed above.

In this question, we can use voice recognition (something you are) and a one-time PIN token (something you have) to provide two factors of authentication. The one-time PIN token is a small device that generates a one-time PIN to enable access.

QUESTION NO: 999

The security administrator notices a user logging into a corporate Unix server remotely as root. Which of the following actions should the administrator take?

- A. Create a firewall rule to block SSH
- B. Delete the root account
- C. Disable remote root logins
- D. Ensure the root account has a strong password

Answer: C

Explanation:

Remote users log in to Unix or Linux servers by using SSH. Although SSH is secure, allowing remote access as root is a security risk.

One of the biggest security holes you could open on a Unix or Linux server is to allow directly logging in as root through SSH, because any cracker can attempt to brute force your root password and potentially get access to your system if they can figure out your password. It's much better to have a separate account that you regularly use and simply sudo to root when necessary.

You should disable root ssh access by editing /etc/ssh/sshd_config to contain:

```
PermitRootLogin no
```

QUESTION NO: 1000

A company plans to expand by hiring new engineers who work in highly specialized areas. Each engineer will have very different job requirements and use unique tools and applications in their job. Which of the following is MOST appropriate to use?

- A.** Role-based privileges
- B.** Credential management
- C.** User assigned privileges
- D.** User access

Answer: A

Explanation:

In this question, we have engineers who require different tools and applications according to their specialized job function. We can therefore use the Role-Based Access Control model.

Role-Based Access Control (RBAC) models approach the problem of access control based on established roles in an organization. RBAC models implement access by job function or by responsibility. Each employee has one or more roles that allow access to specific information. If a person moves from one role to another, the access for the previous role will no longer be available.

Instead of thinking "Denise needs to be able to edit files," RBAC uses the logic "Editors need to be able to edit files" and "Denise is a member of the Editors group." This model is always good for use in an environment in which there is high employee turnover.

QUESTION NO: 1001

A file on a Linux server has default permissions of rw-rw-r--. The system administrator has verified that Ann, a user, is not a member of the group owner of the file. Which of the following should be modified to assure that Ann has read access to the file?

- A.** User ownership information for the file in question

- B. Directory permissions on the parent directory of the file in question
- C. Group memberships for the group owner of the file in question
- D. The file system access control list (FACL) for the file in question

Answer: C

Explanation:

The file permissions according to the file system access control list (FACL) are rw-rw-r--.

The first 'rw-' are the file owner permissions (read and write).

The second 'rw-' are the group permissions (read and write) for the group that has been assigned the file.

The third 'r--' is the All Users permissions; in this case read only.

To enable Ann to access the file, we should add Ann to the group that has been assigned to the file.

Topic 6, Cryptography

QUESTION NO: 1002

Which of the following protocols uses an asymmetric key to open a session and then establishes a symmetric key for the remainder of the session?

- A. SFTP
- B. HTTPS
- C. TFTP
- D. TLS

Answer: D

Explanation:

SSL establishes a session using asymmetric encryption and maintains the session using symmetric encryption.

QUESTION NO: 1003

A company uses PGP to ensure that sensitive email is protected. Which of the following types of cryptography is being used here for the key exchange?

- A. Symmetric
- B. Session-based
- C. Hashing

D. Asymmetric

Answer: A

Explanation:

PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.

QUESTION NO: 1004

Which of the following is true about asymmetric encryption?

- A.** A message encrypted with the private key can be decrypted by the same key
- B.** A message encrypted with the public key can be decrypted with a shared key.
- C.** A message encrypted with a shared key, can be decrypted by the same key.
- D.** A message encrypted with the public key can be decrypted with the private key.

Answer: D

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION NO: 1005

Encryption used by RADIUS is BEST described as:

- A.** Quantum
- B.** Elliptical curve
- C.** Asymmetric
- D.** Symmetric

Answer: D

Explanation:

The RADIUS server uses a symmetric encryption method.

Note: Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected.

QUESTION NO: 1006

Symmetric encryption utilizes _____, while asymmetric encryption utilizes _____.

- A. Public keys, one time
- B. Shared keys, private keys
- C. Private keys, session keys
- D. Private keys, public keys

Answer: D

Explanation:

Symmetrical systems require the key to be private between the two parties. With asymmetric systems, each circuit has one key.

In more detail:

* Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system.

* Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

QUESTION NO: 1007

Users need to exchange a shared secret to begin communicating securely. Which of the following is another name for this symmetric key?

- A. Session Key
- B. Public Key
- C. Private Key
- D. Digital Signature

Answer: C

Explanation:

Symmetric algorithms require both ends of an encrypted message to have the same key and processing algorithms. Symmetric algorithms generate a secret key that must be protected. A symmetric key, sometimes referred to as a secret key or private key, is a key that isn't disclosed to people who aren't authorized to use the encryption system.

QUESTION NO: 1008

In order to securely communicate using PGP, the sender of an email must do which of the following when sending an email to a recipient for the first time?

- A. Import the recipient's public key
- B. Import the recipient's private key
- C. Export the sender's private key
- D. Export the sender's public key

Answer: A

Explanation:

See step 4 below.

1. When a user encrypts plaintext with PGP, PGP first compresses the plaintext.
2. PGP then creates a session key, which is a one-time-only secret key.
3. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext.
4. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

QUESTION NO: 1009

A network stream needs to be encrypted. Sara, the network administrator, has selected a cipher which will encrypt 8 bits at a time before sending the data across the network. Which of the following has Sara selected?

- A. Block cipher
- B. Stream cipher
- C. CRC
- D. Hashing algorithm

Answer: A

Explanation:

With a block cipher the algorithm works on chunks of data—encrypting one and then moving to the next.

Example: Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds.

QUESTION NO: 1010

The concept of rendering data passing between two points over an IP based network impervious to all but the most sophisticated advanced persistent threats is BEST categorized as which of the following?

- A. Stream ciphers
- B. Transport encryption
- C. Key escrow
- D. Block ciphers

Answer: B

Explanation:

Transport encryption is the process of encrypting data ready to be transmitted over an insecure network. A common example of this would be online banking or online purchases where sensitive information such as account numbers or credit card numbers is transmitted.

Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

QUESTION NO: 1011

Which of the following transportation encryption protocols should be used to ensure maximum security between a web browser and a web server?

- A. SSLv2
- B. SSHv1
- C. RSA
- D. TLS

Answer: D

Explanation:

HTTP Secure HTTP Secure (HTTPS) is the protocol used for "secure" web pages that users should see when they must enter personal information such as credit card numbers, passwords, and other identifiers. It combines HTTP with SSL/TLS to provide encrypted communication. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL, and it is also referred to as SSL 3.1.

QUESTION NO: 1012

Which of the following ports should be opened on a firewall to allow for NetBIOS communication? (Select TWO).

- A. 110
- B. 137
- C. 139
- D. 143
- E. 161
- F. 443

Answer: B,C

Explanation: NetBIOS provides four distinct services:

Name service for name registration and resolution (port: 137/udp)

Name service for name registration and resolution (port: 137/tcp)

Datagram distribution service for connectionless communication (port: 138/udp)

Session service for connection-oriented communication (port: 139/tcp)

QUESTION NO: 1013

Which of the following concepts is enforced by certifying that email communications have been sent by who the message says it has been sent by?

- A. Key escrow
- B. Non-repudiation
- C. Multifactor authentication
- D. Hashing

Answer: B

Explanation:

Regarding digital security, the cryptological meaning and application of non-repudiation shifts to mean:

A service that provides proof of the integrity and origin of data.

An authentication that can be asserted to be genuine with high assurance.

QUESTION NO: 1014

All of the following are valid cryptographic hash functions EXCEPT:

- A. RIPEMD.
- B. RC4.
- C. SHA-512.
- D. MD4.

Answer: B

Explanation:

RC4 is not a hash function. RC4 is popular with wireless and WEP/WPA encryption.

QUESTION NO: 1015

Which of the following concepts is used by digital signatures to ensure integrity of the data?

- A. Non-repudiation
- B. Hashing
- C. Transport encryption
- D. Key escrow

Answer: B

Explanation:

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

QUESTION NO: 1016

A security administrator discovers an image file that has several plain text documents hidden in the file. Which of the following security goals is met by camouflaging data inside of other files?

- A. Integrity
- B. Confidentiality
- C. Steganography
- D. Availability

Answer: C

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be

incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION NO: 1017

A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered?

- A. Symmetric encryption
- B. Non-repudiation
- C. Steganography
- D. Hashing

Answer: C

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION NO: 1018

Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?

- A. Hashing
- B. Transport encryption
- C. Digital signatures
- D. Steganography

Answer: D

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION NO: 1019

Which of the following must a user implement if they want to send a secret message to a coworker by embedding it within an image?

- A. Transport encryption
- B. Steganography
- C. Hashing
- D. Digital signature

Answer: B

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION NO: 1020

Digital Signatures provide which of the following?

- A. Confidentiality
- B. Authorization
- C. Integrity
- D. Authentication
- E. Availability

Answer: C

Explanation:

A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender.

QUESTION NO: 1021

Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability?

- A. Twofish
- B. Diffie-Hellman
- C. ECC
- D. RSA

Answer: C**Explanation:**

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size.

QUESTION NO: 1022

Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device?

- A. Block cipher
- B. Elliptical curve cryptography
- C. Diffie-Hellman algorithm
- D. Stream cipher

Answer: B**Explanation:**

Regarding the performance of ECC applications on various mobile devices, ECC is the most suitable PKC (Public-key cryptography) scheme for use in a constrained environment.

Note: Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided

by keys of smaller size. Using smaller key size would be faster.

QUESTION NO: 1023

A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network?

- A. Spoof the MAC address of an observed wireless network client
- B. Ping the access point to discover the SSID of the network
- C. Perform a dictionary attack on the access point to enumerate the WEP key
- D. Capture client to access point disassociation packets to replay on the local PC's loopback

Answer: A

Explanation:

With ARP spoofing (also known as ARP poisoning), the MAC (Media Access Control) address of the data is faked. By faking this value, it is possible to make it look as if the data came from a network that it did not. This can be used to gain access to the network, to fool the router into sending data here that was intended for another host, or to launch a DoS attack. In all cases, the address being faked is an address of a legitimate user, and that makes it possible to get around such measures as allow/deny lists.

Note: As an example, the initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

QUESTION NO: 1024

The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this?

- A. Disable the SSID broadcasting
- B. Configure the access points so that MAC filtering is not used
- C. Implement WEP encryption on the access points
- D. Lower the power for office coverage only

Answer: D

Explanation:

On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided.

QUESTION NO: 1025

Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this?

- A. Disable default SSID broadcasting.
- B. Use WPA instead of WEP encryption.
- C. Lower the access point's power settings.
- D. Implement MAC filtering on the access point.

Answer: D

Explanation:

If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so.

QUESTION NO: 1026

Which of the following provides the strongest authentication security on a wireless network?

- A. MAC filter
- B. WPA2
- C. WEP
- D. Disable SSID broadcast

Answer: B

Explanation:

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

QUESTION NO: 1027

Which of the following is a concern when encrypting wireless data with WEP?

- A. WEP displays the plain text entire key when wireless packet captures are reassembled
- B. WEP implements weak initialization vectors for key transmission
- C. WEP uses a very weak encryption algorithm
- D. WEP allows for only four pre-shared keys to be configured

Answer: B

Explanation:

The initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack.

QUESTION NO: 1028

Which of the following provides the HIGHEST level of confidentiality on a wireless network?

- A. Disabling SSID broadcast
- B. MAC filtering
- C. WPA2
- D. Packet switching

Answer: C

Explanation:

The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP.

QUESTION NO: 1029

While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing?

- A. EAP-TLS
- B. PEAP
- C. WEP
- D. WPA

Answer: C

Explanation:

WEP is one of the more vulnerable security protocols. The only time to use WEP is when you must have compatibility with older devices that do not support new encryption.

QUESTION NO: 1030

Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises.

A security technician was asked to prepare a report of files that had changed since last night's integrity scan.

Which of the following could the technician use to prepare the report? (Select TWO).

- A. PGP
- B. MD5
- C. ECC
- D. AES
- E. Blowfish
- F. HMAC

Answer: B,F

Explanation:

B: MD5 can be used to locate the data which has changed.

The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

F: A common method of verifying integrity involves adding a message authentication code (MAC) to the message.

HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key.

QUESTION NO: 1031

Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them?

- A. Whole disk encryption
- B. SSH
- C. Telnet
- D. MD5

Answer: D

Explanation:

MD5 can be used to locate the data which has changed.

The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.

QUESTION NO: 1032

Which of the following is used to verify data integrity?

- A. SHA
- B. 3DES
- C. AES
- D. RSA

Answer: A

Explanation:

SHA stands for "secure hash algorithm". SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It is used to ensure data integrity.

Note:

A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact. This is how hashing is used to ensure data integrity.

QUESTION NO: 1033

Which of the following can be implemented with multiple bit strength?

- A. AES
- B. DES
- C. SHA-1
- D. MD5
- E. MD4

Answer: A

Explanation:

AES (a symmetric algorithm) uses key sizes of 128, 192, or 256 bits.

QUESTION NO: 1034

To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended?

- A. SHA
- B. MD5
- C. Blowfish
- D. AES

Answer: D

Explanation:

AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is used to encrypt data, not to verify data integrity.

QUESTION NO: 1035

Which of the following provides additional encryption strength by repeating the encryption process with additional keys?

- A. AES
- B. 3DES
- C. TwoFish
- D. Blowfish

Answer: B

Explanation:

Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION NO: 1036

Which of the following are restricted to 64-bit block sizes? (Select TWO).

- A. PGP
- B. DES
- C. AES256
- D. RSA
- E. 3DES
- F. AES

Answer: B,E

Explanation:

B: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's based on a 56-bit key and has several modes that offer security and integrity. It is now considered insecure because of the small key size.

E: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION NO: 1037

A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data?

- A. AES
- B. 3DES
- C. RC4
- D. WPA2

Answer: B

Explanation:

3DES (Triple DES) is based on DES.

In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV). Microsoft OneNote, Microsoft Outlook 2007, and Microsoft System Center Configuration Manager 2012, use Triple DES to password protect user content and system data.

QUESTION NO: 1038

Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible?

- A. ECC**
- B. RSA**
- C. SHA**
- D. 3DES**

Answer: D

Explanation:

3DES would be less secure compared to ECC, but 3DES would require less computational power. Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys).

QUESTION NO: 1039

Which of the following **MUST** Matt, a security administrator, implement to verify both the integrity and authenticity of a message while requiring a shared secret?

- A. RIPEMD**
- B. MD5**
- C. SHA**
- D. HMAC**

Answer: D

Explanation:

HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key. The hashing function provides data integrity, while the symmetric key provides authenticity.

QUESTION NO: 1040

Which of the following cryptographic algorithms is MOST often used with IPSec?

- A. Blowfish
- B. Twofish
- C. RC4
- D. HMAC

Answer: D

Explanation:

The HMAC-MD5-96 (also known as HMAC-MD5) encryption technique is used by IPSec to make sure that a message has not been altered.

QUESTION NO: 1041

When creating a public / private key pair, for which of the following ciphers would a user need to specify the key strength?

- A. SHA
- B. AES
- C. DES
- D. RSA

Answer: D

Explanation:

RSA (an asymmetric algorithm) uses keys of a minimum length of 2048 bits.

QUESTION NO: 1042

Which of the following uses both a public and private key?

- A. RSA
- B. AES
- C. MD5
- D. SHA

Answer: A

Explanation:

The RSA algorithm is an early public-key encryption system that uses large integers as the basis for the process.

RSA uses both a public key and a secret.

RSA key generation process:

1. Generate two large random primes, p and q , of approximately equal size such that their product, $n = pq$, is of the required bit length (such as 2048 bits, 4096 bits, and so forth).

Let $n = pq$

Let $m = (p-1)(q-1)$

2. Choose a small number e , co-prime to m (note: Two numbers are co-prime if they have no common factors).

3. Find d , such that

$de \% m = 1$

4. Publish e and n as the public key. Keep d and n as the secret key.

QUESTION NO: 1043

Which of the following ciphers would be BEST used to encrypt streaming video?

- A. RSA
- B. RC4
- C. SHA1
- D. 3DES

Answer: B

Explanation:

In cryptography, RC4 is the most widely used software stream cipher and is used in popular Internet protocols such as Transport Layer Security (TLS). While remarkable for its simplicity and speed in software, RC4 has weaknesses that argue against its use in new systems. It is especially vulnerable when the beginning of the output keystream is not discarded, or when nonrandom or related keys are used; some ways of using RC4 can lead to very insecure protocols such as WEP.

Because RC4 is a stream cipher, it is more malleable than common block ciphers. If not used together with a strong message authentication code (MAC), then encryption is vulnerable to a bit-flipping attack. The cipher is also vulnerable to a stream cipher attack if not implemented correctly.

Furthermore, inadvertent double encryption of a message with the same key may accidentally output plaintext rather than ciphertext because the involutory nature of the XOR function would result in the second operation reversing the first.

It is noteworthy, however, that RC4, being a stream cipher, was for a period of time the only common cipher that was immune to the 2011 BEAST attack on TLS 1.0. The attack exploits a known weakness in the way cipher block chaining mode is used with all of the other ciphers supported by TLS 1.0, which are all block ciphers.

QUESTION NO: 1044

Due to hardware limitation, a technician must implement a wireless encryption algorithm that uses the RC4 protocol. Which of the following is a wireless encryption solution that the technician should implement while ensuring the STRONGEST level of security?

- A.** WPA2-AES
- B.** 802.11ac
- C.** WPA-TKIP
- D.** WEP

Answer: C

Explanation:

WPA-TKIP uses the RC4 cipher.

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC)

To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key.

QUESTION NO: 1045

A security administrator must implement a wireless encryption system to secure mobile devices' communication. Some users have mobile devices which only support 56-bit encryption. Which of

the following wireless encryption methods should be implemented?

- A. RC4
- B. AES
- C. MD5
- D. TKIP

Answer: A

Explanation:

RC4 is popular with wireless and WEP/WPA encryption. It is a streaming cipher that works with key sizes between 40 and 2048 bits, and it is used in SSL and TLS.

QUESTION NO: 1046

Which of the following can use RC4 for encryption? (Select TWO).

- A. CHAP
- B. SSL
- C. WEP
- D. AES
- E. 3DES

Answer: B,C

Explanation: B: In cryptography, RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4) is the most widely used software stream cipher and is used in popular Internet protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).
C: WEP also uses RC4, however WEP is still unsecure.

QUESTION NO: 1047

Which of the following would provide the STRONGEST encryption?

- A. Random one-time pad
- B. DES with a 56-bit key
- C. AES with a 256-bit key
- D. RSA with a 1024-bit key

Answer: A

Explanation:

One-time pads are the only truly completely secure cryptographic implementations.

They are so secure for two reasons. First, they use a key that is as long as a plaintext message. That means there is no pattern in the key application for an attacker to use. Also, one-time pad keys are used only once and then discarded. So even if you could break a one-time pad cipher, that same key would never be used again, so knowledge of the key would be useless.

QUESTION NO: 1048

Which of the following symmetric key algorithms are examples of block ciphers? (Select THREE).

- A. RC4
- B. 3DES
- C. AES
- D. MD5
- E. PGP
- F. Blowfish

Answer: B,C,F

Explanation:

B: Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

C: Advanced Encryption Standard (AES) is a block cipher that has replaced DES as the current standard, and it uses the Rijndael algorithm. It was developed by Joan Daemen and Vincent Rijmen. AES is the current product used by U.S. governmental agencies.

F: Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds.

QUESTION NO: 1049

Which of the following should be used when a business needs a block cipher with minimal key size for internal encryption?

- A. AES
- B. Blowfish
- C. RC5
- D. 3DES

Answer: B

Explanation:

Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

QUESTION NO: 1050

Sara, a security engineer, is testing encryption ciphers for performance. Which of the following ciphers offers strong encryption with the FASTEST speed?

- A. 3DES
- B. Blowfish
- C. Serpent
- D. AES256

Answer: B

Explanation:

Blowfish is an encryption system invented by a team led by Bruce Schneier that performs a 64-bit block cipher at very fast speeds. Blowfish is a fast, except when changing keys. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits).

QUESTION NO: 1051

Jane, a VPN administrator, was asked to implement an encryption cipher with a MINIMUM effective security of 128-bits. Which of the following should Jane select for the tunnel encryption?

- A. Blowfish
- B. DES
- C. SHA256
- D. HMAC

Answer: A

Explanation:

Blowfish is an encryption system that performs a 64-bit block cipher at very fast speeds. It is a symmetric block cipher that can use variable-length keys (from 32 bits to 448 bits). Among the alternatives listed above, it is the only cipher that can use a 128-bit key and which does provide additional security through a symmetric key.

QUESTION NO: 1052

When using PGP, which of the following should the end user protect from compromise? (Select TWO).

- A. Private key
- B. CRL details
- C. Public key
- D. Key password
- E. Key escrow
- F. Recovery agent

Answer: A,D

Explanation:

A: In PGP only the private key belonging to the receiver can decrypt the session key.

PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key.

D: PGP uses a passphrase to encrypt your private key on your machine. Your private key is encrypted on your disk using a hash of your passphrase as the secret key. You use the passphrase to decrypt and use your private key.

QUESTION NO: 1053

A security administrator must implement a system to allow clients to securely negotiate encryption keys with the company's server over a public unencrypted communication channel.

Which of the following implements the required secure key negotiation? (Select TWO).

- A. PBKDF2
- B. Symmetric encryption
- C. Steganography
- D. ECDHE
- E. Diffie-Hellman

Answer: D,E

Explanation:

Elliptic curve Diffie–Hellman (ECDH) is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel. This shared secret may be directly used as a key, or better yet, to derive another key which can then be used to encrypt subsequent communications using a symmetric

key cipher. It is a variant of the Diffie–Hellman protocol using elliptic curve cryptography.

Note: Adding an ephemeral key to Diffie-Hellman turns it into DHE (which, despite the order of the acronym, stands for Ephemeral Diffie-Hellman).

Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE (again, overlook the order of the acronym letters; it is called Ephemeral Elliptic Curve Diffie-Hellman). It is the ephemeral component of each of these that provides the perfect forward secrecy.

QUESTION NO: 1054

An administrator has two servers and wants them to communicate with each other using a secure algorithm.

Which of the following choose to provide both CRC integrity checks and RCA encryption?

- A. NTLM
- B. RSA
- C. CHAP
- D. ECDHE

Answer: D

Explanation:

ECDHE provides both CRC integrity checks and RCA encryption.

Adding an ephemeral key to Elliptic Curve Diffie-Hellman turns it into ECDHE. It is the ephemeral component of each of these that provides the perfect forward secrecy.

Forward secrecy is a property of any key exchange system, which ensures that if one key is compromised, subsequent keys will not also be compromised. Perfect forward secrecy occurs when this process is unbreakable.

QUESTION NO: 1055

Connections using point-to-point protocol authenticate using which of the following? (Select TWO).

- A. RIPEMD
- B. PAP
- C. CHAP
- D. RC4
- E. Kerberos

Answer: B,C

Explanation:

B: A password authentication protocol (PAP) is an authentication protocol that uses a password. PAP is used by Point to Point Protocol to validate users before allowing them access to server resources.

C: CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake.

QUESTION NO: 1056

Which of the following offers the LEAST secure encryption capabilities?

- A. TwoFish
- B. PAP
- C. NTLM
- D. CHAP

Answer: B

Explanation:

PAP transmits unencrypted ASCII passwords over the network and is therefore considered insecure. It is used as a last resort when the remote server does not support a stronger authentication protocol, like CHAP or EAP.

QUESTION NO: 1057

Which of the following algorithms has well documented collisions? (Select TWO).

- A. AES
- B. MD5
- C. SHA
- D. SHA-256
- E. RSA

Answer: B,C

Explanation:

B: MD5 biggest weakness is that it does not have strong collision resistance, and thus it is no longer recommended for use.

C: SHA-1 (also known as SHA) is being retired from most government uses; the U.S. National Institute of Standards and Technology said, "Federal agencies should stop using SHA-1

for...applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010", though that was later relaxed.

Note: The hashing algorithm must have few or no collisions. This means that hashing two different inputs does not give the same output.

Cryptographic hash functions are usually designed to be collision resistant. But many hash functions that were once thought to be collision resistant were later broken. MD5 and SHA-1 in particular both have published techniques more efficient than brute force for finding collisions.

QUESTION NO: 1058

Which of the following protocols is the security administrator observing in this packet capture?

12:33:43, SRC 192.168.4.3:3389, DST 10.67.33.20:8080, SYN/ACK

- A. HTTPS
- B. RDP
- C. HTTP
- D. SFTP

Answer: B

Explanation:

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

Example of RDP tracing output:

No. Time Delta Source Destination Protocol Length Info

5782, 2013-01-06 09:52:15.407, 0.000, SRC 10.7.3.187, DST 10.0.107.58, TCP, 62, 3389 > 59193 [SYN, ACK]

QUESTION NO: 1059

Which of the following cryptographic related browser settings allows an organization to communicate securely?

- A. SSL 3.0/TLS 1.0
- B. 3DES
- C. Trusted Sites
- D. HMAC

Answer: A

Explanation:

Secure Sockets Layer (SSL) is used to establish a secure communication connection between two TCP-based machines. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default.

QUESTION NO: 1060

Recent data loss on financial servers due to security breaches forced the system administrator to harden their systems. Which of the following algorithms with transport encryption would be implemented to provide the MOST secure web connections to manage and access these servers?

- A. SSL
- B. TLS
- C. HTTP
- D. FTP

Answer: B

Explanation:

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Transport Layer Security (TLS) is a security protocol that expands upon SSL. Many industry analysts predict that TLS will replace SSL in the future. TLS 1.0 was first defined in RFC 2246 in January 1999 as an upgrade of SSL Version 3.0. As of February 2015, the latest versions of all major web browsers support TLS 1.0, 1.1, and 1.2, have them enabled by default.

QUESTION NO: 1061

A security administrator has been tasked with setting up a new internal wireless network that must use end to end TLS. Which of the following may be used to meet this objective?

- A. WPA
- B. HTTPS
- C. WEP
- D. WPA 2

Answer: D

Explanation:

Wi-Fi Protected Access 2 (WPA2) was intended to provide security that's equivalent to that on a wired network, and it implements elements of the 802.11i standard. In April 2010, the Wi-Fi Alliance announced the inclusion of additional Extensible Authentication Protocol (EAP) types to its certification programs for WPA- and WPA2- Enterprise certification programs. EAP-TLS is included in this certification program.

Note: Although WPA mandates the use of TKIP, WPA2 requires Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). CCMP uses 128-bit AES encryption with a 48-bit initialization vector. With the larger initialization vector, it increases the difficulty in cracking and minimizes the risk of a replay attack.

QUESTION NO: 1062

Which of the following protocols encapsulates an IP packet with an additional IP header?

- A. SFTP
- B. IPSec
- C. HTTPS
- D. SSL

Answer: B

Explanation:

Authentication Header (AH) is a member of the IPsec protocol suite. AH operates directly on top of IP, using IP protocol number 51.

QUESTION NO: 1063

A new MPLS network link has been established between a company and its business partner.

The link provides logical isolation in order to prevent access from other business partners. Which of the following should be applied in order to achieve confidentiality and integrity of all data across the link?

- A. MPLS should be run in IPVPN mode.
- B. SSL/TLS for all application flows.
- C. IPSec VPN tunnels on top of the MPLS link.
- D. HTTPS and SSH for all application flows.

Answer: C

Explanation:

IPSec can very well be used with MPLS. IPSec could provide VPN tunnels on top of the MPLS link. Internet Protocol Security (IPSec) isn't a tunneling protocol, but it's used in conjunction with tunneling protocols. IPSec is oriented primarily toward LAN-to-LAN connections, but it can also be used with dial-up connections. IPSec provides secure authentication and encryption of data and headers; this makes it a good choice for security.

QUESTION NO: 1064

Which of the following would be used as a secure substitute for Telnet?

- A. SSH
- B. SFTP
- C. SSL
- D. HTTPS

Answer: A

Explanation:

Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent programs for such Unix standards as Telnet, FTP, and many other communications-oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment.

QUESTION NO: 1065

Which of the following protocols provides transport security for virtual terminal emulation?

- A. TLS
- B. SSH
- C. SCP
- D. S/MIME

Answer: B

Explanation:

Secure Shell (SSH) is a tunneling protocol originally designed for Unix systems. It uses encryption to establish a secure connection between two systems. SSH also provides alternative, security-equivalent programs for such Unix standards as Telnet, FTP, and many other communications-

oriented applications. SSH is available for use on Windows systems as well. This makes it the preferred method of security for Telnet and other cleartext oriented programs in the Unix environment.

QUESTION NO: 1066

A security engineer is asked by the company's development team to recommend the most secure method for password storage.

Which of the following provide the BEST protection against brute forcing stored passwords? (Select TWO).

- A. PBKDF2
- B. MD5
- C. SHA2
- D. Bcrypt
- E. AES
- F. CHAP

Answer: A,D

Explanation:

A: PBKDF2 (Password-Based Key Derivation Function 2) is part of PKCS #5 v. 2.01. It applies some function (like a hash or HMAC) to the password or passphrase along with Salt to produce a derived key.

D: bcrypt is a key derivation function for passwords based on the Blowfish cipher. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function: over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.

The bcrypt function is the default password hash algorithm for BSD and many other systems.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, pp. 109-110, 139, 143, 250, 255-256, 256

QUESTION NO: 1067

Deploying a wildcard certificate is one strategy to:

- A. Secure the certificate's private key.
- B. Increase the certificate's encryption key length.
- C. Extend the renewal date of the certificate.
- D. Reduce the certificate management burden.

Answer: D

Explanation:

A wildcard certificate is a public key certificate which can be used with multiple subdomains of a domain. This saves money and reduces the management burden of managing multiple certificates, one for each subdomain.

A single Wildcard certificate for *.example.com, will secure all these domains:

payment.example.com

contact.example.com

login-secure.example.com

www.example.com

Because the wildcard only covers one level of subdomains (the asterisk doesn't match full stops), these domains would not be valid for the certificate:

test.login.example.com

QUESTION NO: 1068

A certificate authority takes which of the following actions in PKI?

- A. Signs and verifies all infrastructure messages
- B. Issues and signs all private keys
- C. Publishes key escrow lists to CRLs
- D. Issues and signs all root certificates

Answer: D

Explanation:

A certificate authority can issue multiple certificates in the form of a tree structure. A root certificate is part of a public key infrastructure (PKI) scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).

Note: In cryptography and computer security, a root certificate is an unsigned public key certificate (also called self-signed certificate) that identifies the Root Certificate Authority (CA).

QUESTION NO: 1069

Which of the following is used to certify intermediate authorities in a large PKI deployment?

- A. Root CA
- B. Recovery agent
- C. Root user
- D. Key escrow

Answer: A

Explanation:

The root CA certifies other certification authorities to publish and manage certificates within the organization.

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree. .

QUESTION NO: 1070

Which of the following components **MUST** be trusted by all parties in PKI?

- A. Key escrow
- B. CA
- C. Private key
- D. Recovery key

Answer: B

Explanation:

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. In a simple trust model all parties must trust the CA.

In a more complicated trust model all parties must trust the Root CA.

QUESTION NO: 1071

Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login. Which of the following is **MOST** likely the issue?

- A. The IP addresses of the clients have change
- B. The client certificate passwords have expired on the server
- C. The certificates have not been installed on the workstations
- D. The certificates have been installed on the CA

Answer: C

Explanation:

The computer certificates must be installed on the upgraded client computers.

QUESTION NO: 1072

A company's security administrator wants to manage PKI for internal systems to help reduce costs. Which of the following is the FIRST step the security administrator should take?

- A. Install a registration server.
- B. Generate shared public and private keys.
- C. Install a CA
- D. Establish a key escrow policy.

Answer: C

Explanation:

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. When you implement a PKI you should start by installing a CA.

QUESTION NO: 1073

Pete, an employee, needs a certificate to encrypt data. Which of the following would issue Pete a certificate?

- A. Certification authority
- B. Key escrow
- C. Certificate revocation list
- D. Registration authority

Answer: A

Explanation:

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates.

QUESTION NO: 1074

When reviewing a digital certificate for accuracy, which of the following would Matt, a security administrator, focus on to determine who affirms the identity of the certificate owner?

- A. Trust models
- B. CRL
- C. CA
- D. Recovery agent

Answer: C

Explanation:

A certificate authority (CA) is an organization that is responsible for issuing, revoking, and distributing certificates. The CA affirms the identity of the certificate owner.

QUESTION NO: 1075

Joe, a user, reports to the system administrator that he is receiving an error stating his certificate has been revoked. Which of the following is the name of the database repository for these certificates?

- A. CSR
- B. OCSP
- C. CA
- D. CRL

Answer: D

Explanation:

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

QUESTION NO: 1076

A systems administrator has implemented PKI on a classified government network. In the event that a disconnect occurs from the primary CA, which of the following should be accessible locally from every site to ensure users with bad certificates cannot gain access to the network?

- A. A CRL

- B. Make the RA available
- C. A verification authority
- D. A redundant CA

Answer: A

Explanation:

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked.

QUESTION NO: 1077

A CRL is comprised of.

- A. Malicious IP addresses.
- B. Trusted CA's.
- C. Untrusted private keys.
- D. Public keys.

Answer: D

Explanation:

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked.

The certificates for which a CRL should be maintained are often X.509/public key certificates, as this format is commonly used by PKI schemes.

QUESTION NO: 1078

Which of the following **MUST** be updated immediately when an employee is terminated to prevent unauthorized access?

- A. Registration
- B. CA
- C. CRL
- D. Recovery agent

Answer: C

Explanation:

Certificates or keys for the terminated employee should be put in the CRL.

A certificate revocation list (CRL) is created and distributed to all CAs to revoke a certificate or key.

By checking the CRL you can check if a particular certificate has been revoked.

QUESTION NO: 1079

Which of the following provides a static record of all certificates that are no longer valid?

- A. Private key
- B. Recovery agent
- C. CRLs
- D. CA

Answer: C

Explanation:

The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release. When a potential user attempts to access a server, the server allows or denies access based on the CRL entry for that particular user.

QUESTION NO: 1080

A CA is compromised and attacks start distributing maliciously signed software updates. Which of the following can be used to warn users about the malicious activity?

- A. Key escrow
- B. Private key verification
- C. Public key verification
- D. Certificate revocation list

Answer: D

Explanation:

If we put the root certificate of the comprised CA in the CRL, users will know that this CA (and the certificates that it has issued) no longer can be trusted.

The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In

addition, each list contains a proposed date for the next release.

QUESTION NO: 1081

The finance department works with a bank which has recently had a number of cyber attacks. The finance department is concerned that the banking website certificates have been compromised. Which of the following can the finance department check to see if any of the bank's certificates are still valid?

- A. Bank's CRL
- B. Bank's private key
- C. Bank's key escrow
- D. Bank's recovery agent

Answer: A

Explanation:

The finance department can check if any of the bank's certificates are in the CRL or not. If a certificate is not in the CRL then it is still valid.

The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

QUESTION NO: 1082

A security administrator needs a locally stored record to remove the certificates of a terminated employee. Which of the following describes a service that could meet these requirements?

- A. OCSP
- B. PKI
- C. CA
- D. CRL

Answer: D

Explanation:

A CRL is a locally stored record containing revoked certificates and revoked keys.

QUESTION NO: 1083

Public key certificates and keys that are compromised or were issued fraudulently are listed on which of the following?

- A. PKI
- B. ACL
- C. CA
- D. CRL

Answer: D

Explanation:

A CRL is a locally stored record containing revoked certificates and revoked keys.

QUESTION NO: 1084

Which of the following identifies certificates that have been compromised or suspected of being compromised?

- A. Certificate revocation list
- B. Access control list
- C. Key escrow registry
- D. Certificate authority

Answer: A

Explanation:

Certificates that have been compromised or are suspected of being compromised are revoked.

A CRL is a locally stored record containing revoked certificates and revoked keys.

QUESTION NO: 1085

When employees that use certificates leave the company they should be added to which of the following?

- A. PKI
- B. CA
- C. CRL
- D. TKIP

Answer: C

Explanation:

The certificates of the leaving employees must be made unusable. This is done by revoking them. The revoke certificates end up in the CRL.

Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included. In addition, each list contains a proposed date for the next release.

QUESTION NO: 1086

Which of the following should a security technician implement to identify untrusted certificates?

- A. CA
- B. PKI
- C. CRL
- D. Recovery agent

Answer: C

Explanation:

Untrusted certificates and keys are revoked and put into the CRL.

Note: The CRL (Certificate revocation list) is exactly what its name implies: a list of subscribers paired with digital certificate status. The list enumerates revoked certificates along with the reason(s) for revocation. The dates of certificate issue, and the entities that issued them, are also included.

QUESTION NO: 1087

Which of the following is true about the CRL?

- A. It should be kept public
- B. It signs other keys
- C. It must be kept secret
- D. It must be encrypted

Answer: A

Explanation:

The CRL must be public so that it can be known which keys and certificates have been revoked. In the operation of some cryptosystems, usually public key infrastructures (PKIs), a certificate revocation list (CRL) is a list of certificates (or more specifically, a list of serial numbers for

certificates) that have been revoked, and therefore, entities presenting those (revoked) certificates should no longer be trusted.

QUESTION NO: 1088

A system administrator is notified by a staff member that their laptop has been lost. The laptop contains the user's digital certificate. Which of the following will help resolve the issue? (Select TWO).

- A. Revoke the digital certificate
- B. Mark the key as private and import it
- C. Restore the certificate using a CRL
- D. Issue a new digital certificate
- E. Restore the certificate using a recovery agent

Answer: A,D

Explanation:

The user's certificate must be revoked to ensure that the stolen computer cannot access resources the user has had access to.

To grant the user access to the resources he must be issued a new certificate.

QUESTION NO: 1089

Which of the following protocols is used to validate whether trust is in place and accurate by returning responses of either "good", "unknown", or "revoked"?

- A. CRL
- B. PKI
- C. OCSP
- D. RA

Answer: C

Explanation:

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.

An OCSP responder (a server typically run by the certificate issuer) may return a signed response signifying that the certificate specified in the request is 'good', 'revoked', or 'unknown'. If it cannot process the request, it may return an error code.

QUESTION NO: 1090

An administrator needs to renew a certificate for a web server. Which of the following should be submitted to a CA?

- A. CSR
- B. Recovery agent
- C. Private key
- D. CRL

Answer: A

Explanation:

In public key infrastructure (PKI) systems, a certificate signing request (also CSR or certification request) is a message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

When you renew a certificate you send a CSR to the CA to get the certificate resigned.

QUESTION NO: 1091

An administrator needs to submit a new CSR to a CA. Which of the following is a valid FIRST step?

- A. Generate a new private key based on AES.
- B. Generate a new public key based on RSA.
- C. Generate a new public key based on AES.
- D. Generate a new private key based on RSA.

Answer: D

Explanation:

Before creating a CSR, the applicant first generates a key pair, keeping the private key secret. The private key is needed to produce, but it is not part of, the CSR.

The private key is an RSA key. The private encryption key that will be used to protect sensitive information.

Note: A CSR or Certificate Signing request is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private key is usually created at the same time that you create the CSR.

QUESTION NO: 1092

In which of the following scenarios is PKI LEAST hardened?

- A. The CRL is posted to a publicly accessible location.
- B. The recorded time offsets are developed with symmetric keys.
- C. A malicious CA certificate is loaded on all the clients.
- D. All public keys are accessed by an unauthorized user.

Answer: C

Explanation:

A rogue Certification Authority (CA) certificate allows malicious users to impersonate any Web site on the Internet, including banking and e-commerce sites secured using the HTTPS protocol. A rogue CA certificate would be seen as trusted by Web browsers, and it is harmful because it can appear to be signed by one of the root CAs that browsers trust by default. A rogue Certification Authority (CA) certificate can be created using a vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure Web sites.

QUESTION NO: 1093

Which of the following BEST describes part of the PKI process?

- A. User1 decrypts data with User2's private key
- B. User1 hashes data with User2's public key
- C. User1 hashes data with User2's private key
- D. User1 encrypts data with User2's public key

Answer: D

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key.

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

You want to send an encrypted message to Jordan, so you request his public key.

Jordan responds by sending you that key.

You use the public key he sends you to encrypt the message.

You send the message to him.

Jordan uses his private key to decrypt the message.

QUESTION NO: 1094

A software development company wants to implement a digital rights management solution to protect its intellectual property. Which of the following should the company implement to enforce software digital rights?

- A. Transport encryption
- B. IPsec
- C. Non-repudiation
- D. Public key infrastructure

Answer: D

Explanation:

The Public-Key Infrastructure (PKI) is intended to offer a means of providing security to messages and transactions on a grand scale. The need for universal systems to support e-commerce, secure transactions, and information privacy is one aspect of the issues being addressed with PKI. A PKI can be used to protect software.

QUESTION NO: 1095

Which of the following is the MOST likely cause of users being unable to verify a single user's email signature and that user being unable to decrypt sent messages?

- A. Unmatched key pairs
- B. Corrupt key escrow
- C. Weak public key
- D. Weak private key

Answer: A

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. The sender and receiver must have a matching key in order for the receiver to decrypt the data.

QUESTION NO: 1096

In PKI, a key pair consists of: (Select TWO).

- A. A key ring
- B. A public key
- C. A private key
- D. Key escrow
- E. A passphrase

Answer: B,C

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key. The key pair consists of these two keys.

QUESTION NO: 1097

Which of the following is true about PKI? (Select TWO).

- A. When encrypting a message with the public key, only the public key can decrypt it.
- B. When encrypting a message with the private key, only the private key can decrypt it.
- C. When encrypting a message with the public key, only the CA can decrypt it.
- D. When encrypting a message with the public key, only the private key can decrypt it.
- E. When encrypting a message with the private key, only the public key can decrypt it.

Answer: D,E

Explanation:

E: You encrypt data with the private key and decrypt with the public key, though the opposite is much more frequent.

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

D: In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key.

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

You want to send an encrypted message to Jordan, so you request his public key.

Jordan responds by sending you that key.

You use the public key he sends you to encrypt the message.

You send the message to him.

Jordan uses his private key to decrypt the message.

QUESTION NO: 1098

Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

- A. Recovery agent
- B. Certificate authority
- C. Trust model
- D. Key escrow

Answer: A

Explanation:

If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

QUESTION NO: 1099

Pete, an employee, is terminated from the company and the legal department needs documents from his encrypted hard drive. Which of the following should be used to accomplish this task? (Select TWO).

- A. Private hash
- B. Recovery agent
- C. Public key
- D. Key escrow
- E. CRL

Answer: B,D

Explanation:

B: If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

D: If a key need to be recovered for legal purposes the key escrow can be used.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

QUESTION NO: 1100

After encrypting all laptop hard drives, an executive officer's laptop has trouble booting to the operating system. Now that it is successfully encrypted the helpdesk cannot retrieve the data.

Which of the following can be used to decrypt the information for retrieval?

- A. Recovery agent
- B. Private key
- C. Trust models
- D. Public key

Answer: A

Explanation:

To access the data the hard drive need to be decrypted. To decrypt the hard drive you would need the proper private key. The key recovery agent can retrieve the required key.

A key recovery agent is an entity that has the ability to recover a key, key components, or plaintext messages as needed.

QUESTION NO: 1101

Which of the following is true about the recovery agent?

- A. It can decrypt messages of users who lost their private key.
- B. It can recover both the private and public key of federated users.
- C. It can recover and provide users with their lost or private key.
- D. It can recover and provide users with their lost public key.

Answer: A

Explanation:

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted

data.

QUESTION NO: 1102

The recovery agent is used to recover the:

- A. Root certificate
- B. Key in escrow
- C. Public key
- D. Private key

Answer: D

Explanation:

A key recovery agent is an entity that has the ability to recover a private key, key components, or plaintext messages as needed. Using the recovered key the recovery agent can decrypt encrypted data.

QUESTION NO: 1103

Which of the following is synonymous with a server's certificate?

- A. Public key
- B. CRL
- C. Private key
- D. Recovery agent

Answer: A

Explanation:

A public key certificate (also known as a digital certificate or identity certificate) is an electronic document used to prove ownership of a public key.

QUESTION NO: 1104

The security administrator installed a newly generated SSL certificate onto the company web server. Due to a misconfiguration of the website, a downloadable file containing one of the pieces of the key was available to the public. It was verified that the disclosure did not require a reissue of the certificate. Which of the following was MOST likely compromised?

- A. The file containing the recovery agent's keys.
- B. The file containing the public key.
- C. The file containing the private key.
- D. The file containing the server's encrypted passwords.

Answer: B

Explanation:

The public key can be made available to everyone. There is no need to reissue the certificate.

QUESTION NO: 1105

The public key is used to perform which of the following? (Select THREE).

- A. Validate the CRL
- B. Validate the identity of an email sender
- C. Encrypt messages
- D. Perform key recovery
- E. Decrypt messages
- F. Perform key escrow

Answer: B,C,E

Explanation:

B: The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

C: The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message.

E: You encrypt data with the private key and decrypt with the public key, though the opposite is much more frequent.

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public. Although different, the two parts of this key pair are mathematically linked.

QUESTION NO: 1106

Public keys are used for which of the following?

- A. Decrypting wireless messages
- B. Decrypting the hash of an electronic signature
- C. Bulk encryption of IP based email traffic
- D. Encrypting web browser traffic

Answer: B

Explanation:

The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

QUESTION NO: 1107

Which of the following explains the difference between a public key and a private key?

- A. The public key is only used by the client while the private key is available to all. Both keys are mathematically related.
- B. The private key only decrypts the data while the public key only encrypts the data. Both keys are mathematically related.
- C. The private key is commonly used in symmetric key decryption while the public key is used in asymmetric key decryption.
- D. The private key is only used by the client and kept secret while the public key is available to all.

Answer: D

Explanation:

The private key must be kept secret at all time. The private key is only by the client. The public key is available to anybody.

QUESTION NO: 1108

Ann wants to send a file to Joe using PKI. Which of the following should Ann use in order to sign the file?

- A. Joe's public key
- B. Joe's private key
- C. Ann's public key
- D. Ann's private key

Answer: D

Explanation:

The sender uses his private key, in this case Ann's private key, to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

The receiver uses a key provided by the sender—the public key—to decrypt the message.

Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidentally, in transit.

QUESTION NO: 1109

Which of the following devices is BEST suited for servers that need to store private keys?

- A. Hardware security module
- B. Hardened network firewall
- C. Solid state disk drive
- D. Hardened host firewall

Answer: A

Explanation:

A hardware security module (HSM) is a physical computing device that safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

By adding a HSM to the server and storing the private keys on HSM, the security of the keys would be improved.

QUESTION NO: 1110

Company A sends a PGP encrypted file to company B. If company A used company B's public key to encrypt the file, which of the following should be used to decrypt data at company B?

- A. Registration
- B. Public key
- C. CRLs
- D. Private key

Answer: D

Explanation:

In a PKI the sender encrypts the data using the receiver's public key. The receiver decrypts the data using his own private key.

PKI is a two-key, asymmetric system with four main components: certificate authority (CA), registration authority (RA), RSA (the encryption algorithm), and digital certificates. Messages are encrypted with a public key and decrypted with a private key.

A PKI example:

You want to send an encrypted message to Jordan, so you request his public key.

Jordan responds by sending you that key.

You use the public key he sends you to encrypt the message.

You send the message to him.

Jordan uses his private key to decrypt the message.

QUESTION NO: 1111

Which of the following is true about an email that was signed by User A and sent to User B?

- A.** User A signed with User B's private key and User B verified with their own public key.
- B.** User A signed with their own private key and User B verified with User A's public key.
- C.** User A signed with User B's public key and User B verified with their own private key.
- D.** User A signed with their own public key and User B verified with User A's private key.

Answer: B

Explanation:

The sender uses his private key, in this case User A's private key, to create a digital signature.

The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The receiver (User B) uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic.

The receiver uses a key provided by the sender—the public key—to decrypt the message.

QUESTION NO: 1112

Which of the following must be kept secret for a public key infrastructure to remain secure?

- A.** Certificate Authority
- B.** Certificate revocation list
- C.** Public key ring
- D.** Private key

Answer: D

Explanation:

The private key, which is also called the secret key, must be kept secret.

QUESTION NO: 1113

Which of the following allows an organization to store a sensitive PKI component with a trusted third party?

- A. Trust model
- B. Public Key Infrastructure
- C. Private key
- D. Key escrow

Answer: D

Explanation:

Sensitive PKI data, such as private keys, can be put into key escrow data. The key escrow data can be kept at a trusted third party.

Key escrow is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

QUESTION NO: 1114

Which of the following is a requirement when implementing PKI if data loss is unacceptable?

- A. Web of trust
- B. Non-repudiation
- C. Key escrow
- D. Certificate revocation list

Answer: C

Explanation:

Key escrow is a database of stored keys that later can be retrieved.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages) and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

QUESTION NO: 1115

Which of the following allows lower level domains to access resources in a separate Public Key Infrastructure?

- A. Trust Model
- B. Recovery Agent
- C. Public Key
- D. Private Key

Answer: A

Explanation:

In a bridge trust model allows lower level domains to access resources in a separate PKI through the root CA.

A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate.

In a bridge trust model, a peer-to-peer relationship exists among the root CAs. The root CAs can communicate with one another, allowing cross certification. This arrangement allows a certification process to be established between organizations or departments.

Each intermediate CA trusts only the CAs above and below it, but the CA structure can be expanded without creating additional layers of CAs.

QUESTION NO: 1116

A network administrator is looking for a way to automatically update company browsers so they import a list of root certificates from an online source. This online source will then be responsible for tracking which certificates are to be trusted or not trusted. Which of the following BEST describes the service that should be implemented to meet these requirements?

- A. Trust model
- B. Key escrow
- C. OCSP
- D. PKI

Answer: A

Explanation:

In this scenario we can put a CA in the local network and use an online CA as root CA in a hierarchical trust model.

A trust Model is collection of rules that informs application on how to decide the legitimacy of a

Digital Certificate.

In a hierarchical trust model, also known as a tree, a root CA at the top provides all of the information. The intermediate CAs are next in the hierarchy, and they trust only information provided by the root CA. The root CA also trusts intermediate CAs that are in their level in the hierarchy and none that aren't. This arrangement allows a high level of control at all levels of the hierarchical tree.

QUESTION NO: 1117

In order to use a two-way trust model the security administrator **MUST** implement which of the following?

- A.** DAC
- B.** PKI
- C.** HTTPS
- D.** TPM

Answer: B

Explanation:

PKI is a high level concept. Within a PKI you use a trust model to set up trust between Certification Authorities (CAs).

A public key infrastructure (PKI) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

QUESTION NO: 1118

Which of the following types of trust models is used by a PKI?

- A.** Transitive
- B.** Open source
- C.** Decentralized
- D.** Centralized

Answer: D

Explanation:

PKI uses a centralized trust model. In a simple PKI a single centralized certification authority (CA). In a hierarchical trust model the root CA is the center of the model, with subordinate CAs lower in the hierarchy.

Note: A public key infrastructure (PKI) is a set of hardware, software, people, policies, and

procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate.

QUESTION NO: 1119

RC4 is a strong encryption protocol that is generally used with which of the following?

- A. WPA2 CCMP
- B. PEAP
- C. WEP
- D. EAP-TLS

Answer: C

Explanation:

Rivest Cipher 4 (RC4) is a 128-bit stream cipher used WEP and WPA encryption.

QUESTION NO: 1120

A security administrator must implement a secure key exchange protocol that will allow company clients to autonomously exchange symmetric encryption keys over an unencrypted channel.

Which of the following MUST be implemented?

- A. SHA-256
- B. AES
- C. Diffie-Hellman
- D. 3DES

Answer: C

Explanation:

Diffie-Hellman key exchange (D-H) is a means of securely generating symmetric encryption keys across an insecure medium.

QUESTION NO: 1121

A security administrator at a company which implements key escrow and symmetric encryption only, needs to decrypt an employee's file. The employee refuses to provide the decryption key to the file. Which of the following can the administrator do to decrypt the file?

- A. Use the employee's private key
- B. Use the CA private key
- C. Retrieve the encryption key
- D. Use the recovery agent

Answer: C

Explanation:

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee's private messages have been called into question.

QUESTION NO: 1122

A system administrator is setting up a file transfer server. The goal is to encrypt the user authentication and the files the user is sending using only a user ID and a key pair. Which of the following methods would achieve this goal?

- A. AES
- B. IPSec
- C. PGP
- D. SSH

Answer: D

Explanation:

With SSH you can use automatically generated public-private key pairs to encrypt a network connection, and then use password authentication to log on. Or you can use a manually generated public-private key pair to perform the authentication, allowing users or programs to log in without having to specify a password.

QUESTION NO: 1123

Joe, a user, wants to protect sensitive information stored on his hard drive. He uses a program that encrypted the whole hard drive. Once the hard drive is fully encrypted, he uses the same program to create a hidden volume within the encrypted hard drive and stores the sensitive information within the hidden volume. This is an example of which of the following? (Select TWO).

- A. Multi-pass encryption
- B. Transport encryption

- C. Plausible deniability
- D. Steganography
- E. Transitive encryption
- F. Trust models

Answer: C,D

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video. In this case, it is a hidden volume within the encrypted hard drive. In cryptography, deniable encryption may be used to describe steganographic techniques, where the very existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that an encrypted message exists. This then provides you with plausible deniability.

QUESTION NO: 1124

A company is concerned that a compromised certificate may result in a man-in-the-middle attack against backend financial servers. In order to minimize the amount of time a compromised certificate would be accepted by other servers, the company decides to add another validation step to SSL/TLS connections. Which of the following technologies provides the FASTEST revocation capability?

- A. Online Certificate Status Protocol (OCSP)
- B. Public Key Cryptography (PKI)
- C. Certificate Revocation Lists (CRL)
- D. Intermediate Certificate Authority (CA)

Answer: A

Explanation:

CRL (Certificate Revocation List) was first released to allow the CA to revoke certificates, however due to limitations with this method it was succeeded by OCSP. The main advantage to OCSP is that because the client is allowed query the status of a single certificate, instead of having to download and parse an entire list there is much less overhead on the client and network.

QUESTION NO: 1125

A technician wants to verify the authenticity of the system files of a potentially compromised system. Which of the following can the technician use to verify if a system file was compromised? (Select TWO).

- A. AES

- B. PGP
- C. SHA
- D. MD5
- E. ECDHE

Answer: C,D

Explanation:

Hashing is used to prove the integrity of data to prove that it hasn't been modified. Hashing algorithms are used to derive a key mathematically from a message. The most common hashing standards for cryptographic applications are the SHA and MD algorithms.

QUESTION NO: 1126

When confidentiality is the primary concern, and a secure channel for key exchange is not available, which of the following should be used for transmitting company documents?

- A. Digital Signature
- B. Symmetric
- C. Asymmetric
- D. Hashing

Answer: C

Explanation:

Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. Asymmetric algorithms do not require a secure channel for the initial exchange of secret keys between the parties.

QUESTION NO: 1127

A small company wants to employ PKI. The company wants a cost effective solution that must be simple and trusted. They are considering two options: X.509 and PGP. Which of the following would be the BEST option?

- A. PGP, because it employs a web-of-trust that is the most trusted form of PKI.
- B. PGP, because it is simple to incorporate into a small environment.
- C. X.509, because it uses a hierarchical design that is the most trusted form of PKI.
- D. X.509, because it is simple to incorporate into a small environment.

Answer: B

Explanation:

PGP easier to use and setup than the corporate PKI model, but it is also less robust when it comes to issues like authentication and trust. However, the full benefits of public key cryptography are used.

QUESTION NO: 1128

Which of the following represents a cryptographic solution where the encrypted stream cannot be captured by a sniffer without the integrity of the stream being compromised?

- A. Elliptic curve cryptography.
- B. Perfect forward secrecy.
- C. Steganography.
- D. Quantum cryptography.

Answer: D

Explanation:

Quantum cryptography is a cryptosystem that is completely secure against being compromised without knowledge of the sender or the receiver of the messages.

QUESTION NO: 1129

A new client application developer wants to ensure that the encrypted passwords that are stored in their database are secure from cracking attempts. To implement this, the developer implements a function on the client application that hashes passwords thousands of times prior to being sent to the database. Which of the following did the developer MOST likely implement?

- A. RIPEMD
- B. PBKDF2
- C. HMAC
- D. ECDHE

Answer: B

Explanation:

Password-Based Key Derivation Function 2 (PBKDF2) makes use of a hashing operation, an encryption cipher function, or an HMAC operation) on the input password, which is combined with a salt and is repeated thousands of times.

QUESTION NO: 1130

Joe must send Ann a message and provide Ann with assurance that he was the actual sender. Which of the following will Joe need to use to BEST accomplish the objective?

- A. A pre-shared private key
- B. His private key
- C. Ann's public key
- D. His public key

Answer: B

Explanation:

To achieve both authentication and confidentiality, Joe should include Ann's name in the message, sign it using his private key, and then encrypt both the message and the signature using Ann's public key.

QUESTION NO: 1131

A system administrator wants to confidentially send a user name and password list to an individual outside the company without the information being detected by security controls. Which of the following would BEST meet this security goal?

- A. Digital signatures
- B. Hashing
- C. Full-disk encryption
- D. Steganography

Answer: D

Explanation:

Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.

Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

QUESTION NO: 1132

Protecting the confidentiality of a message is accomplished by encrypting the message with which of the following?

- A. Sender's private key
- B. Recipient's public key
- C. Sender's public key
- D. Recipient's private key

Answer: B

Explanation:

To achieve both authentication and confidentiality, the sender should include the recipient's name in the message, sign it using his private key, and then encrypt both the message and the signature using the recipient's public key.

Topic 7, Mixed Questions

QUESTION NO: 1133

A software developer utilizes cryptographic functions to generate codes that verify message integrity. Due to the nature of the data that is being sent back and forth from the client application to the server, the developer would like to change the cryptographic function to one that verifies both authentication and message integrity. Which of the following algorithms should the software developer utilize?

- A. HMAC
- B. SHA
- C. Two Fish
- D. RIPEMD

Answer: D

Explanation:

QUESTION NO: 1134

When designing a corporate NAC solution, which of the following is the MOST relevant integration issue?

- A. Infrastructure time sync

- B. End user mobility
- C. 802.1X supplicant compatibility
- D. Network Latency
- E. Network Zoning

Answer: D

Explanation:

QUESTION NO: 1135

Which of the following access methods uses radio frequency waves for authentication?

- A. Video surveillance
- B. Mantraps
- C. Proximity readers
- D. Biometrics

Answer: C

Explanation:

QUESTION NO: 1136

Which of the following authentication methods can use the SCTP and TLS protocols for reliable packet transmissions?

- A. TACACS+
- B. SAML
- C. Diameter
- D. Kerberos

Answer: C

Explanation:

QUESTION NO: 1137

Which of the following authentication protocols makes use of UDP for its services?

- A. RADIUS

- B. TACACS+
- C. LDAP
- D. XTACACS

Answer: A

Explanation:

QUESTION NO: 1138

Which of the following is considered a risk management BEST practice of succession planning?

- A. Reducing risk of critical information being known to an individual person who may leave the organization
- B. Implementing company-wide disaster recovery and business continuity plans
- C. Providing career advancement opportunities to junior staff which reduces the possibility of insider threats
- D. Considering departmental risk management practices in place of company-wide practices

Answer: B

Explanation:

QUESTION NO: 1139

Which of the following is the BEST technology for the sender to use in order to secure the in-band exchange of a shared key?

- A. Steganography
- B. Hashing algorithm
- C. Asymmetric cryptography
- D. Steam cipher

Answer: C

Explanation:

QUESTION NO: 1140

Which of the following design components is used to isolate network devices such as web servers?

- A. VLAN
- B. VPN
- C. NAT
- D. DMZ

Answer: D

Explanation:

QUESTION NO: 1141

Which of the following is MOST critical in protecting control systems that cannot be regularly patched?

- A. Asset inventory
- B. Full disk encryption
- C. Vulnerability scanning
- D. Network segmentation

Answer: B

Explanation:

QUESTION NO: 1142

Identifying residual is MOST important to which of the following concepts?

- A. Risk deterrence
- B. Risk acceptance
- C. Risk mitigation
- D. Risk avoidance

Answer: C

Explanation:

QUESTION NO: 1143

Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?

- A. Preshared keys
- B. Ticket exchange
- C. Initialization vectors
- D. Certificate exchange

Answer: B

Explanation:

QUESTION NO: 1144

Which of the following steps of incident response does a team analyze the incident and determine steps to prevent a future occurrence?

- A. Mitigation
- B. Identification
- C. Preparation
- D. Lessons learned

Answer: D

Explanation:

QUESTION NO: 1145

A technician wants to secure communication to the corporate web portal, which is currently using HTTP. Which of the following is the FIRST step the technician should take?

- A. Send the server's public key to the CA
- B. Install the CA certificate on the server
- C. Import the certificate revocation list into the server
- D. Generate a certificate request from the server

Answer: D

Explanation:

QUESTION NO: 1146

An organization has a need for security control that identifies when an organizational system has been unplugged and a rouge system has been plugged in. The security control must also provide the ability to supply automated notifications. Which of the following would allow the organization to

BEST meet this business requirement?

- A. MAC filtering
- B. ACL
- C. SNMP
- D. Port security

Answer: D

Explanation:

QUESTION NO: 1147

Internet banking customers currently use an account number and password to access their online accounts. The bank wants to improve security on high value transfers by implementing a system which call users back on a mobile phone to authenticate the transaction with voice verification. Which of the following authentication factors are being used by the bank?

- A. Something you know, something you do, and something you have
- B. Something you do, somewhere you are, and something you have
- C. Something you are, something you do and something you know
- D. Something you have, something you are, and something you know

Answer: C

Explanation:

QUESTION NO: 1148

A security administrator has concerns that employees are installing unapproved applications on their company provide smartphones. Which of the following would BEST mitigate this?

- A. Implement remote wiping user acceptance policies
- B. Disable removable storage capabilities
- C. Implement an application whitelist
- D. Disable the built-in web browsers

Answer: C

Explanation:

QUESTION NO: 1149

The security manager must store a copy of a sensitive document and needs to verify at a later point that the document has not been altered. Which of the following will accomplish the security manager's objective?

- A. RSA
- B. AES
- C. MD5
- D. SHA

Answer: C

Explanation:

QUESTION NO: 1150

A security Operations Center was scanning a subnet for infections and found a contaminated machine. One of the administrators disabled the switch port that the machine was connected to, and informed a local technician of the infection. Which of the following steps did the administrator perform?

- A. Escalation
- B. Identification
- C. Notification
- D. Quarantine
- E. Preparation

Answer: C,D

Explanation:

QUESTION NO: 1151

A security administrator wants to block unauthorized access to a web server using a locally installed software program. Which of the following should the administrator deploy?

- A. NIDS
- B. HIPS
- C. NIPS
- D. HIDS

Answer: B

Explanation:**QUESTION NO: 1152**

A network administrator has identified port 21 being open and the lack of an IDS as a potential risk to the company. Due to budget constraints, FTP is the only option that the company can is to transfer data and network equipment cannot be purchased. Which of the following is this known as?

- A. Risk transference
- B. Risk deterrence
- C. Risk acceptance
- D. Risk avoidance

Answer: C

Explanation:

QUESTION NO: 1153

A security administrator is investigating a recent server breach. The breach occurred as a result of a zero-day attack against a user program running on the server. Which of the following logs should the administrator search for information regarding the breach?

- A. Application log
- B. Setup log
- C. Authentication log
- D. System log

Answer: A

Explanation:

QUESTION NO: 1154

A user attempts to install new and relatively unknown software recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

- A. Application black listing
- B. Network Intrusion Prevention System
- C. Group policy
- D. Application white listing

Answer: A

Explanation:

QUESTION NO: 1155

A system administrator is configuring shared secrets on servers and clients. Which of the following authentication services is being deployed by the administrator? (Select two.)

- A. Kerberos
- B. RADIUS
- C. TACACS+
- D. LDAP
- E. Secure LDAP

Answer: B,D

Explanation:

QUESTION NO: 1156

The finance department just procured a software application that needs to communicate back to the vendor server via SSL. Which of the following default ports on the firewall must the security engineer open to accomplish this task?

- A. 80
- B. 130
- C. 443
- D. 3389

Answer: C

Explanation:

QUESTION NO: 1157

After an audit, it was discovered that an account was not disabled in a timely manner after an

employee has departed from the organization. Which of the following did the organization fail to properly implement?

- A. Routine account audits
- B. Account management processes
- C. Change management processes
- D. User rights and permission reviews

Answer: A

Explanation:

QUESTION NO: 1158

The Chief Security Officer (CSO) for a datacenter in a hostile environment is concerned about protecting the facility from car bomb attacks. Which of the following BEST would protect the building from this threat? (Select two.)

- A. Dogs
- B. Fencing
- C. CCTV
- D. Guards
- E. Bollards
- F. Lighting

Answer: B,E

Explanation:

QUESTION NO: 1159

Users can authenticate to a company's web applications using their credentials from a popular social media site. Which of the following poses the greatest risk with this integration?

- A. Malicious users can exploit local corporate credentials with their social media credentials
- B. Changes to passwords on the social media site can be delayed from replicating to the company
- C. Data loss from the corporate servers can create legal liabilities with the social media site
- D. Password breaches to the social media affect the company application as well

Answer: D

Explanation:

QUESTION NO: 1160

A corporation has experienced several media leaks of proprietary data on various web forums. The posts were made during business hours and it is believed that the culprit is posting during work hours from a corporate machine. The Chief Information Officer (CIO) wants to scan internet traffic and keep records for later use in legal proceedings once the culprit is found. Which of the following provides the BEST solution?

- A. Protocol analyzer
- B. NIPS
- C. Proxy server
- D. HIDS

Answer: A

Explanation:

QUESTION NO: 1161

The security administrator runs an rpm verify command which records the MD5 sum, permissions, and timestamp of each file on the system. The administrator saves this information to a separate server. Which of the following describes the procedure the administrator has performed?

- A. Host software base-lining
- B. File snapshot collection
- C. TPM
- D. ROMDB verification

Answer: D

Explanation:

QUESTION NO: 1162

Users are trying to communicate with a network but are unable to do so. A network administrator sees connection attempts on port 20 from outside IP addresses that are being blocked. How can the administrator resolve this?

- A. Enable stateful FTP on the firewall
- B. Enable inbound SSH connections

- C. Enable NETBIOS connections in the firewall
- D. Enable HTTPS on port 20

Answer: A

Explanation:

QUESTION NO: 1163

In order to enter a high-security datacenter, users are required to speak the password into a voice recognition system. Ann a member of the sales department over hears the password and upon speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

- A. An authentication factor
- B. Discretionary access
- C. Time of day restrictions
- D. Least privilege restrictions

Answer: A

Explanation:

QUESTION NO: 1164

Given the following list of corporate access points, which of the following attacks is MOST likely underway if the company wireless network uses the same wireless hardware throughout?

MACSID

- 00:01:AB:FA:CD:34Corporate AP
- 00:01:AB:FA:CD:35Corporate AP
- 00:01:AB:FA:CD:36Corporate AP
- 00:01:AB:FA:CD:37Corporate AP
- 00:01:AB:FA:CD:34Corporate AP

- A. Packet sniffing
- B. Evil Twin
- C. WPS attack
- D. Rogue access point

Answer: B

Explanation:

QUESTION NO: 1165

A system administrator has noticed network performance issues and wants to gather performance data from the gateway router. Which of the following can be used to perform this action?

- A. SMTP
- B. iSCSI
- C. SNMP
- D. IPSec

Answer: C

Explanation:

QUESTION NO: 1166

Which of the following technologies was developed to allow companies to use less-expensive storage while still maintaining the speed and redundancy required in a business environment?

- A. RAID
- B. Tape Backup
- C. Load Balancing
- D. Clustering

Answer: D

Explanation:

QUESTION NO: 1167

An employee needs to connect to a server using a secure protocol on the default port. Which of the following ports should be used?

- A. 21
- B. 22
- C. 80
- D. 110

Answer: B

Explanation:

QUESTION NO: 1168

Which of the following is replayed during wireless authentication to exploit a weak key infrastructure?

- A. Preshared keys
- B. Ticket exchange
- C. Initialization vectors
- D. Certificate exchange

Answer: B

Explanation:

QUESTION NO: 1169

A new security policy being implemented requires all email within the organization be digitally signed by the author using PGP. Which of the following would need to be created for each user?

- A. A certificate authority
- B. A key escrow
- C. A trusted key
- D. A public and private key

Answer: A

Explanation:

QUESTION NO: 1170

Which of the following authentication provides users XML for authorization and authentication?

- A. Kerberos
- B. LDAP
- C. RADIUS
- D. SAML

Answer: D

Explanation:

QUESTION NO: 1171

A company wants to prevent end users from plugging unapproved smartphones into PCs and transferring data. Which of the following would be the BEST control to implement?

- A. MDM
- B. IDS
- C. DLP
- D. HIPS

Answer: C

Explanation:

QUESTION NO: 1172

The ore-sales engineering team needs to quickly provide accurate and up-to-date information to potential clients. This information includes design specifications and engineering data that is developed and stored using numerous applications across the enterprise. Which of the following authentication technique is MOST appropriate?

- A. Common access cards
- B. TOTP
- C. Single sign-on
- D. HOTP

Answer: B

Explanation:

QUESTION NO: 1173

A network engineer is configuring a VPN tunnel connecting a company's network to a business partner. Which of the following protocols should be used for key exchange?

- A. SHA-1
- B. RC4

- C. Blowfish
- D. Diffie-Hellman

Answer: A

Explanation:

QUESTION NO: 1174

Which of the following types of cloud computing would be MOST appropriate if an organization required complete control of the environment?

- A. Hybrid Cloud
- B. Private cloud
- C. Community cloud
- D. Community cloud
- E. Public cloud

Answer: B

Explanation:

QUESTION NO: 1175

The database server used by the payroll system crashed at 3 PM and payroll is due at 5 PM. Which of the following metrics is MOST important in this instance?

- A. ARO
- B. SLE
- C. MTTR
- D. MTBF

Answer: C

Explanation:

QUESTION NO: 1176

Which of the following is an attack designed to activate based on time?

- A. Logic Bomb

- B. Backdoor
- C. Trojan
- D. Rootkit

Answer: A

Explanation:

QUESTION NO: 1177

A network security engineer notices unusual traffic on the network from a single IP attempting to access systems on port 23. Port 23 is not used anywhere on the network. Which of the following should the engineer do to harden the network from this type of intrusion in the future?

- A. Disable unnecessary services on servers
- B. Disable unused accounts on servers and network devices
- C. Implement password requirements on servers and network devices
- D. Enable auditing on event logs

Answer: A

Explanation:

QUESTION NO: 1178

Which of the following documents outlines the responsibility of both participants in an agreement between two organizations?

- A. RFC
- B. MOU
- C. RFQ
- D. SLA

Answer: B

Explanation:

QUESTION NO: 1179

Users in the HR department were recently informed that they need to implement a user training and awareness program which is tailored to their department. Which of the following types of training would be the MOST appropriate for this department?

- A. Handling PII
- B. Risk mitigation
- C. Input validation
- D. Hashing

Answer: A

Explanation:

QUESTION NO: 1180

Which of the following incident response plan steps would MOST likely engaging business professionals with the security team to discuss changes to existing procedures?

- A. Recovery
- B. Incident identification
- C. Isolation / quarantine
- D. Lessons learned
- E. Reporting

Answer: D

Explanation:

QUESTION NO: 1181

A company is starting to allow employees to use their own personal without centralized management. Employees must contract IT to have their devices configured to use corporate email; access is also available to the corporate cloud-based services. Which of the following is the BEST policy to implement under these circumstances?

- A. Acceptable use policy
- B. Security policy
- C. Group policy
- D. Business Agreement policy

Answer: A

Explanation:

QUESTION NO: 1182

Which of the following BEST explains Platform as a Service?

- A. An external entity that provides a physical or virtual instance of an installed operating system
- B. A third party vendor supplying support services to maintain physical platforms and servers
- C. An external group providing operating systems installed on virtual servers with web applications
- D. An internal group providing physical server instances without installed operating systems or support

Answer: C

Explanation:

QUESTION NO: 1183

One of the senior managers at a company called the help desk to report to report a problem. The manager could no longer access data on a laptop equipped with FDE. The manager requested that the FDE be removed and the laptop restored from a backup. The help desk informed the manager that the recommended solution was to decrypt the hard drive prior to reinstallation and recovery. The senior manager did not have a copy of the private key associated with the FDE on the laptop. Which of the following tools or techniques did the help desk use to avoid losing the data on the laptop?

- A. Public key
- B. Recovery agent
- C. Registration details
- D. Trust Model

Answer: B

Explanation:

QUESTION NO: 1184

An employee in the accounting department recently received a phishing email that instructed them to click a link in the email to view an important message from the IRS which threatened penalties if a response was not received by the end of the business day. The employee clicked on the link and the machine was infected with malware. Which of the following principles BEST describes why this social engineering ploy was successful?

- A. Scarcity
- B. Familiarity
- C. Social proof

D. Urgency

Answer: A

Explanation:

QUESTION NO: 1185

A security technician received notification of a remotely exploitable vulnerability affecting all multifunction printers firmware installed throughout the organization. The vulnerability allows a malicious user to review all the documents processed by the affected printers. Which of the following compensating controls can the security technician to mitigate the security risk of a sensitive document leak?

- A. Create a separate printer network**
- B. Perform penetration testing to rule out false positives**
- C. Install patches on the print server**
- D. Run a full vulnerability scan of all the printers**

Answer: C

Explanation:

QUESTION NO: 1186

A systems administrator has made several unauthorized changes to the server cluster that resulted in a major outage. This event has been brought to the attention of the Chief Information Office (CIO) and he has requested immediately implement a risk mitigation strategy to prevent this type of event from reoccurring. Which of the following would be the BEST risk mitigation strategy to implement in order to meet this request?

- A. Asset Management**
- B. Change Management**
- C. Configuration Management**
- D. Incident Management**

Answer: B

Explanation:

QUESTION NO: 1187

An incident occurred when an outside attacker was able to gain access to network resources. During the incident response, investigation security logs indicated multiple failed login attempts for a network administrator. Which of the following controls, if in place could have BEST prevented this successful attack?

- A. Password history
- B. Password complexity
- C. Account lockout
- D. Account expiration

Answer: C

Explanation:

QUESTION NO: 1188

Joe needs to track employees who log into a confidential database and edit files. In the past, critical files have been edited, and no one admits to making the edits. Which of the following does Joe need to implement in order to enforce accountability?

- A. Non-repudiation
- B. Fault tolerance
- C. Hashing
- D. Redundancy

Answer: C

Explanation:

QUESTION NO: 1189

A new mobile banking application is being developed and uses SSL / TLS certificates but penetration tests show that it is still vulnerable to man-in-the-middle attacks, such as DNS hijacking. Which of the following would mitigate this attack?

- A. Certificate revocation
- B. Key escrow
- C. Public key infrastructure
- D. Certificate pinning

Answer: D

Explanation:

QUESTION NO: 1190

One month after a software developer was terminated the helpdesk started receiving calls that several employees' computers were being infected with malware. Upon further research, it was determined that these employees had downloaded a shopping toolbar. It was this toolbar that downloaded and installed the errant code. Which of the following attacks has taken place?

- A. Logic bomb
- B. Cross-site scripting
- C. SQL injection
- D. Malicious add-on

Answer: A

Explanation:

QUESTION NO: 1191

Which of the following would an attacker use to penetrate and capture additional traffic prior to performing an IV attack?

- A. DNS poisoning
- B. DDoS
- C. Replay attack
- D. Dictionary attacks

Answer: D

Explanation:

QUESTION NO: 1192

An administrator has concerns regarding the company's server rooms Proximity badge readers were installed, but it is discovered this is not preventing unapproved personnel from tailgating into these area. Which of the following would BEST address this concern?

- A. Replace proximity readers with turn0based key locks
- B. Install man-traps at each restricted area entrance
- C. Configure alarms to alert security when the areas are accessed

D. Install monitoring cameras at each entrance

Answer: B

Explanation:

QUESTION NO: 1193

Which of the following would be a reason for developers to utilize an AES cipher in CCM mode (Counter with Chain Block Message Authentication Code)?

- A. It enables the ability to reverse the encryption with a separate key
- B. It allows for one time pad inclusions with the passphrase
- C. Counter mode alternates between synchronous and asynchronous encryption
- D. It allows a block cipher to function as a stream cipher

Answer: D

Explanation:

QUESTION NO: 1194

One of the findings of risk assessment is that many of the servers on the data center subnet contain data that is in scope for PCI compliance, Everyone in the company has access to these servers, regardless of their job function. Which of the following should the administrator do?

- A. Segment the network
- B. Use 802.1X
- C. Deploy a proxy sever
- D. Configure ACLs
- E. Write an acceptable use policy

Answer: A

Explanation:

QUESTION NO: 1195

Various employees have lost valuable customer data due to hard drives failing in company provided laptops. It has been discovered that the hard drives used in one model of laptops provided by the company has been recalled by the manufactory, The help desk is only able to replace the hard drives after they fail because there is no centralized records of the model of

laptop given to each specific user. Which of the following could have prevented this situation from occurring?

- A. Data backups
- B. Asset tracking
- C. Support ownership
- D. BYOD policies

Answer: A

Explanation:

QUESTION NO: 1196

Attempting to inject 50 alphanumeric key strokes including spaces into an application input field that only expects four alpha characters is considered which of the following attacks?

- A. XML injection
- B. Buffer overflow
- C. LDAP Injection
- D. SQL injection

Answer: D

Explanation:

QUESTION NO: 1197

An organization is required to log all user internet activity. Which of the following would accomplish this requirement?

- A. Configure an access list on the default gateway router. Configure the default gateway router to log all web traffic to a syslog server
- B. Configure a firewall on the internal network. On the client IP address configuration, use the IP address of the firewall as the default gateway, configure the firewall to log all traffic to a syslog server
- C. Configure a proxy server on the internal network and configure the proxy server to log all web traffic to a syslog server
- D. Configure an access list on the core switch, configure the core switch to log all web traffic to a syslog server

Answer: C

Explanation:

QUESTION NO: 1198

An agent wants to create fast and efficient cryptographic keys to use with Diffie-Hellman without using prime numbers to generate the keys. Which of the following should be used?

- A. Elliptic curve cryptography
- B. Quantum cryptography
- C. Public key cryptography
- D. Symmetric cryptography

Answer: D

Explanation:

QUESTION NO: 1199

Joe an application developer is building an external facing marketing site. There is an area on the page where clients may submit their feedback to articles that are posted. Joe filters client-side JAVA input. Which of the following is Joe attempting to prevent?

- A. SQL injections
- B. Watering holes
- C. Cross site scripting
- D. Pharming

Answer: C

Explanation:

QUESTION NO: 1200

A video surveillance audit recently uncovered that an employee plugged in a personal laptop and used the corporate network to browse inappropriate and potentially malicious websites after office hours. Which of the following could BEST prevent a situation like this from occurring again?

- A. Intrusion detection
- B. Content filtering
- C. Port security

D. Vulnerability scanning

Answer: C

Explanation:

QUESTION NO: 1201

A server administrator notes that a fully patched application often stops running due to a memory error. When reviewing the debugging logs they notice code being run calling an internal process to exploit the machine. Which of the following attacks does this describes?

- A. Malicious add-on
- B. SQL injection
- C. Cross site scripting
- D. Zero-day

Answer: D

Explanation:

QUESTION NO: 1202

A resent OS patch caused an extended outage. It took the IT department several hours to uncover the cause of the issue due to the system owner who installed the patch being out of the office. Which of the following could help reduce the likelihood of this situation occurring in the future?

- A. Separation of duties
- B. Change management procedures
- C. Incident management procedures
- D. User rights audits and reviews

Answer: B

Explanation:

QUESTION NO: 1203

The Chief Information Security Officer (CISO) is concerned that users could bring their personal laptops to work and plug them directly into the network port under their desk. Which of the following should be configured on the network switch to prevent this from happening?

- A. Access control lists
- B. Loop protection
- C. Firewall rule
- D. Port security

Answer: D

Explanation:

QUESTION NO: 1204

Ann a network administrator has been tasked with strengthening the authentication of users logging into systems in area containing sensitive information. Users log in with usernames and passwords, following by a retinal scan. Which of the following could she implement to add an additional factor of authorization?

- A. Requiring PII usage
- B. Fingerprint scanner
- C. Magnetic swipe cards
- D. Complex passphrases

Answer: B

Explanation:

QUESTION NO: 1205

In an environment where availability is critical such as Industrial control and SCADA networks, which of the following technologies in the MOST critical layer of defense for such systems?

- A. Log consolidation
- B. Intrusion Prevention system
- C. Automated patch deployment
- D. Antivirus software

Answer: B

Explanation:

QUESTION NO: 1206

A security manager installed a standalone fingerprint reader at the data center. All employees that

need to access the data center have been enrolled to the reader and local reader database is always kept updates. When an employee who has been enrolled uses the fingerprint reader the door to the data center opens. Which of the following does this demonstrate? (Select THREE)

- A. Two-factor authentication
- B. Single sign-on
- C. Something you have
- D. Identification
- E. Authentication
- F. Authorization

Answer: A,D,E

Explanation:

QUESTION NO: 1207

A network technician is configuring clients for VLAN access. The network address for the sales department is 192.168.0.64 with a broadcast address of 192.168.0.71. Which of the following IP address/subnet mask combinations could be used to correctly configure a client machine in the sales department?

- A. 192.168.0.64/29
- B. 192.168.0.66/27
- C. 192.168.0.67/29
- D. 192.168.0.70/28

Answer: A

Explanation:

QUESTION NO: 1208

The help desk is experiencing a higher than normal amount of calls from users reporting slow response from the application server. After analyzing the data from a packet capturing tool, the head of the network engineering department determines that the issue is due, in part from the increase of personnel recently hired to perform application development. Which of the following would BEST assist in correcting this issue?

- A. Load balancer
- B. Spam filter
- C. VPN Concentrator

D. NIDS

Answer: A

Explanation:

QUESTION NO: 1209

Two organizations want to share sensitive data with one another from their IT systems to support a mutual customer base. Both organizations currently have secure network and security policies and procedures. Which of the following should be the PRIMARY security considerations by the security managers at each organization prior to sharing information? (Select THREE)

- A. Physical security controls**
- B. Device encryption**
- C. Outboarding/Offboarding**
- D. Use of digital signatures**
- E. SLA/ISA**
- F. Data ownership**
- G. Use of smartcards or common access cards**
- H. Patch management**

Answer: B,E,F

Explanation:

QUESTION NO: 1210

A company's password and authentication policies prohibit the use of shared passwords and transitive trust. Which of the following if implemented would violate company policy? (Select TWO)

- A. Discretionary access control**
- B. Federation**
- C. Single sign-on**
- D. TOTP**
- E. Two-factor authentication**

Answer: A,C

Explanation:

QUESTION NO: 1211

Which of the following types of attacks is based on coordinating small slices of a task across multiple systems?

- A. DDos
- B. Spam
- C. Spoofing
- D. Dos

Answer: B

Explanation:

QUESTION NO: 1212

A system security analyst wants to capture data flowing in and out of the enterprise. Which of the following would MOST likely help in achieving this goal?

- A. Taking screenshots
- B. Analyzing Big Data metadata
- C. Analyzing network traffic and logs
- D. Capturing system image

Answer: C

Explanation:

QUESTION NO: 1213

The security manager reports that the process of revoking certificates authority is too slow and should be automated. Which of the following should be used to automate this process?

- A. CRL
- B. GPG
- C. OCSP
- D. Key escrow

Answer: C

Explanation:

QUESTION NO: 1214

A user attempts to install a new and relatively unknown software program recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

- A. Application black listing
- B. Network Intrusion Prevention System
- C. Group Policy
- D. Application White Listing

Answer: A

Explanation:

QUESTION NO: 1215

A company needs to provide web-based access to shared data sets to mobile users, while maintaining a standardized set of security controls. Which of the following technologies is the MOST appropriate storage?

- A. Encrypted external hard drives
- B. Cloud storage
- C. Encrypted mobile devices
- D. Storage Area Network

Answer: B

Explanation:

QUESTION NO: 1216

An employee's mobile device associates with the company's guest WiFi SSID, but then is unable to retrieve email. The email settings appear to be correct. Which of the following is the MOST likely cause?

- A. The employee has set the network type to WPA instead of WPA2
- B. The network uses a captive portal and requires a web authentication
- C. The administrator has blocked the use of the personal hot spot feature
- D. The mobile device has been placed in airplane mode

Answer: B

Explanation:**QUESTION NO: 1217**

A malicious individual used an unattended customer service kiosk in a busy store to change the prices of several products. The alteration was not noticed until several days later and resulted in the loss of several thousand dollars for the store. Which of the following would BEST prevent this from occurring again?

- A. Password expiration
- B. Screen locks
- C. Inventory control
- D. Asset tracking

Answer: B

Explanation:**QUESTION NO: 1218**

In order to enter a high-security data center, users are required to speak the correct password into a voice recognition system. Ann, a member of the sales department, overhears the password and later speaks it into the system. The system denies her entry and alerts the security team. Which of the following is the MOST likely reason for her failure to enter the data center?

- A. An authentication factor
- B. Discretionary Access
- C. Time of Day Restrictions
- D. Least Privilege Restrictions

Answer: A

Explanation:**QUESTION NO: 1219**

A company requires that all users enroll in the corporate PKI structure and digitally sign all emails. Which of the following are primary reasons to sign emails with digital certificates? (Select TWO)

- A. To establish non-repudiation

- B. To ensure integrity
- C. To prevent SPAM
- D. To establish data loss prevention
- E. To protect confidentiality
- F. To establish transport encryption

Answer: B,E

Explanation:

QUESTION NO: 1220

The Chief Information Officer (CIO) has asked a security analyst to determine the estimated costs associated with each potential breach of their database that contains customer information. Which of the following is the risk calculation that the CIO is asking for?

- A. Impact
- B. SLE
- C. ARO
- D. ALE

Answer: B

Explanation:

QUESTION NO: 1221

A security assurance officer is preparing a plan to measure the technical state of a customer's enterprise. The testers employed to perform the audit will be given access to the customer facility and network. The testers will not be given access to the details of custom developed software used by the customer. However the testers will have access to the source code for several open source applications and pieces of networking equipment used at the facility, but these items will not be within the scope of the audit. Which of the following BEST describes the appropriate method of testing or technique to use in this scenario? (Select TWO)

- A. Social engineering
- B. All source
- C. Black box
- D. Memory dumping
- E. Penetration

Answer: C,E

Explanation:

QUESTION NO: 1222

Which of the following authentication services combines authentication and authorization in a use profile and use UDP?

- A. LDAP
- B. Kerberos
- C. TACACS+
- D. RADIUS

Answer: D

Explanation:

QUESTION NO: 1223

A security administrator is designing an access control system, with an unlimited budget, to allow authenticated users access to network resources. Given that a multifactor authentication solution is more secure, which of the following is the BEST combination of factors?

- A. Retina scanner, thumbprint scanner, and password
- B. Username and password combo, voice recognition scanner, and retina scanner
- C. Password, retina scanner, and proximity reader
- D. One-time password pad, palm-print scanner, and proximity photo badges

Answer: B

Explanation:

QUESTION NO: 1224

The access control list (ACL) for a file on a server is as follows:

User: rwx

User: Ann: r- -

User: Joe: r- -

Group: rwx

Group: sales: r-x

Other: r-x

Joe and Ann are members of the Human Resources group. Will Ann and Joe be able to run the file?

- A. No since Ann and Joe are members of the Sales group owner of the file
- B. Yes since the regular permissions override the ACL for the file
- C. No since the ACL overrides the regular permissions for the file
- D. Yes since the regular permissions and the ACL combine to create the effective permissions on the file

Answer: C

Explanation:

QUESTION NO: 1225

Using a protocol analyzer, a security consultant was able to capture employee's credentials. Which of the following should the consultant recommend to the company, in order to mitigate the risk of employees credentials being captured in the same manner in the future?

- A. Wiping of remnant data
- B. Hashing and encryption of data in-use
- C. Encryption of data in-transit
- D. Hashing of data at-rest

Answer: B

Explanation:

QUESTION NO: 1226

A Company has recently identified critical systems that support business operations. Which of the following will once defined, be the requirement for restoration of these systems within a certain period of time?

- A. Mean Time Between Failure
- B. Mean Time to Restore
- C. Recovery Point Objective
- D. Recovery Time Objective

Answer: A

Explanation:

QUESTION NO: 1227

The software developer is responsible for writing the code and promoting from the development network to the quality network. The network administrator is responsible for promoting code to the application servers. Which of the following practices are they following to ensure application integrity?

- A. Job rotation
- B. Implicit deny
- C. Least privilege
- D. Separation of duties

Answer: D

Explanation:

QUESTION NO: 1228

Ann is traveling for business and is attempting to use the hotel's wireless network to check for new messages. She selects the hotel's wireless SSID from a list of networks and successfully connects. After opening her email client and waiting a few minutes, the connection times out. Which of the following should Ann do to retrieve her email messages?

- A. Change the authentication method for her laptop's wireless card from WEP to WPA2
- B. Open a web browser and authenticate using the captive portal for the hotel's wireless network
- C. Contact the front desk and have the MAC address of her laptop added to the MAC filter on the hotel's wireless network
- D. Change the incoming email protocol from IMAP to POP3

Answer: B

Explanation:

QUESTION NO: 1229

Which of the following password attacks involves attempting all kinds of keystroke combinations on the keyboard with the intention to gain administrative access?

- A. Dictionary
- B. Hybrid
- C. Watering hole
- D. Brute Force

Answer: A

Explanation:

QUESTION NO: 1230

Ann, a security administrator, is strengthening the security controls of the company's campus. Her goal is to prevent people from accessing open locations that are not supervised, such as around the receiving dock. She is also concerned that employees are using these entry points as a way of bypassing the security guard at the main entrance. Which of the following should Ann recommend that would BEST address her concerns?

- A. Increase the lighting surrounding every building on campus
- B. Build fences around campus with gate entrances
- C. Install cameras to monitor the unsupervised areas
- D. Construct bollards to prevent vehicle entry in non-supervised areas

Answer: B

Explanation:

QUESTION NO: 1231

While at an Internet café a malicious user is causing all surrounding wireless connected devices to have intermittent and unstable connections to the access point. Which of the following is MOST likely being used?

- A. Evil Twin
- B. Interference
- C. Packet sniffer
- D. Rogue AP

Answer: D

Explanation:

QUESTION NO: 1232

A password audit has revealed that a significant percentage of end-users have passwords that are easily cracked. Which of the following is the BEST technical control that could be implemented to reduce the amount of easily "crackable" passwords in use?

- A. Credential management
- B. Password history
- C. Password complexity
- D. Security awareness training

Answer: C

Explanation:

QUESTION NO: 1233

While working on a new project a security administrator wants to verify the integrity of the data in the organizations archive library. Which of the following is the MOST secure combination to implement to meet this goal? (Select TWO)

- A. Hash with SHA
- B. Encrypt with Diffie-Hellman
- C. Hash with MD5
- D. Hash with RIPEMD
- E. Encrypt with AES

Answer: C,D

Explanation:

QUESTION NO: 1234

A company has been attacked and their website has been altered to display false information. The security administrator disables the web server service before restoring the website from backup. An audit was performed on the server and no other data was altered. Which of the following should be performed after the server has been restored?

- A. Monitor all logs for the attacker's IP
- B. Block port 443 on the web server
- C. Install and configure SSL to be used on the web server
- D. Configure the web server to be in VLAN 0 across the network

Answer: B

Explanation:

QUESTION NO: 1235

A security administrator suspects that an employee in the IT department is utilizing a reverse proxy to bypass the company's content filter and browse unapproved and non-work related sites while at work. Which of the following tools could BEST be used to determine how the employee is connecting to the reverse proxy?

- A. Port scanner
- B. Vulnerability scanner
- C. Honeypot
- D. Protocol analyzer

Answer: C

Explanation:

QUESTION NO: 1236

Joe, a company's network engineer, is concerned that protocols operating at the application layer of the OSI model are vulnerable to exploitation on the network. Which of the following protocols should he secure?

- A. SNMP
- B. SSL
- C. ICMP
- D. NetBIOS

Answer: A

Explanation:

QUESTION NO: 1237

Ann a security technician receives a report from a user that is unable to access an offsite SSN server. Ann checks the firewall and sees the following rules:

Allow TCP 80

Allow TCP 443

Deny TCP 23

Deny TCP 20

Deny TCP 21

Which of the following is preventing the users from accessing the SSH server?

- A. Deny TCP 20
- B. Deny TCP 21
- C. Deny TCP 23
- D. Implicit deny

Answer: D

Explanation:

QUESTION NO: 1238

An administrator uses a server with a trusted OS and is configuring an application to go into production tomorrow. In order to make a new application work properly, the administrator creates a new policy that labels the application and assigns it a security context within the trusted OS. Which of the following control methods is the administrator using by configuring this policy?

- A. Time based access control
- B. Mandatory access control
- C. Role based access control
- D. Rule based access control

Answer: C

Explanation:

QUESTION NO: 1239

A security administrator has been tasked with assisting in the forensic investigation of an incident relating to employee misconduct. The employee's supervisor believes evidence of this misconduct can be found on the employee's assigned workstation. Which of the following choices BEST describes what should be done? (Select TWO)

- A. Record time as offset as required and conduct a timeline analysis

- B. Update antivirus definitions and conduct a full scan for infected files
- C. Analyze network traffic, system, and file logs
- D. Create an additional local admin account on that workstation to conduct work from
- E. Delete other user profiles on the system to help narrow down the search space
- F. Patch the system before reconnecting it to the network

Answer: A,C

Explanation:

QUESTION NO: 1240

Joe a web developer wants to make sure his application is not susceptible to cross-site request forgery attacks. Which of the following is one way to prevent this type of attack?

- A. The application should always check the HTTP referrer header
- B. The application should always check the HTTP Request header
- C. The application should always check the HTTP Host header
- D. The application should always use SSL encryption

Answer: D

Explanation:

QUESTION NO: 1241

A security technician has been tasked with opening ports on a firewall to allow users to browse the internet. Which of the following ports should be opened on the firewall? (Select Three)

- A. 22
- B. 53
- C. 80
- D. 110
- E. 443
- F. 445
- G. 8080

Answer: C,E,G

Explanation:

QUESTION NO: 1242

A rogue programmer included a piece of code in an application to cause the program to halt at 2:00 PM on Monday afternoon when the application is most utilized. This is Which of the following types of malware?

- A. Trojan
- B. Virus
- C. Logic Bomb
- D. Botnets

Answer: C

Explanation:

QUESTION NO: 1243

After connecting to the corporate network a user types the URL of a popular social media website in the browser but reports being redirected to a login page with the corporate logo. Which of the following is this an example of?

- A. LEAP
- B. MAC filtering
- C. WPA2-Enterprise
- D. Captive portal

Answer: D

Explanation:

QUESTION NO: 1244

The Quality Assurance team is testing a third party application. They are primarily testing for defects and have some understanding of how the application works. Which of the following is the team performing?

- A. Grey box testing
- B. White box testing
- C. Penetration testing
- D. Black box testing

Answer: A

Explanation:

QUESTION NO: 1245

A user Ann has her assigned token but she forgotten her password. Which of the following appropriately categorizes the authentication factor that will fail in this scenario?

- A. Something you do
- B. Something you know
- C. Something you are
- D. Something you have

Answer: B

Explanation:

QUESTION NO: 1246

An employee from the fire Marshall's office arrives to inspect the data center. The operator allows him to bypass the multi-factor authentication to enter the data center. Which of the following types of attacks may be underway?

- A. Impersonation
- B. Hoax
- C. Tailgating
- D. Spoofing

Answer: C

Explanation:

QUESTION NO: 1247

A company recently received accreditation for a secure network, In the accreditation letter, the auditor specifies that the company must keep its security plan current with changes in the network and evolve the systems to adapt to new threats. Which of the following security controls will BEST achieve this goal?

- A. Change management
- B. Group Policy

- C. Continuous monitoring
- D. Credential management

Answer: D

Explanation:

QUESTION NO: 1248

A cyber security administrator receives a list of IPs that have been reported as attempting to access the network. To identify any possible successful attempts across the enterprise, which of the following should be implemented?

- A. Monitor authentication logs
- B. Disable unnecessary accounts
- C. Time of day restrictions
- D. Separation of duties

Answer: A

Explanation:

QUESTION NO: 1249

Which of the following exploits either a host file on a target machine or vulnerabilities on a DNS server in order to carry out URL redirection?

- A. Pharming
- B. Spoofing
- C. Vishing
- D. Phishing

Answer: B

Explanation:

QUESTION NO: 1250

Ann a new small business owner decides to implement WiFi access for her customers. There are several other businesses nearby who also have WiFi hot spots. Ann is concerned about security of the wireless network and wants to ensure that only her customers have access. Which of the following choices BEST meets her intent of security and access?

- A. Enable port security
- B. Enable WPA
- C. Disable SSID broadcasting
- D. Enable WEP

Answer: B

Explanation:

QUESTION NO: 1251

A security engineer is tasked with encrypting corporate email. Which of the following technologies provide the MOST complete protection? (Select TWO)

- A. PGP/GPG
- B. S/MIME
- C. IPSEC
- D. Secure POP3
- E. IMAP
- F. HMAC

Answer: B,F

Explanation:

QUESTION NO: 1252

Which of the following is the GREATEST security concern of allowing employees to bring in their personally owned tablets and connecting to the corporate network?

- A. Tablet network connections are stored and accessible from the corporate network
- B. The company's attack surface increases with the non-corporate devices
- C. Personally purchased media may be available on the network for others to stream
- D. Encrypted tablets are harder to access to determine if they are infected

Answer: C

Explanation:

QUESTION NO: 1253

Searching for systems infected with malware is considered to be which of the following phases of

incident response?

- A. Containment
- B. Preparation
- C. Mitigation
- D. Identification

Answer: D

Explanation:

QUESTION NO: 1254

A technician has deployed a new VPN concentrator. The device needs to authenticate users based on a backend directory service. Which of the following services could be run on the VPN concentrator to perform this authentication?

- A. Kerberos
- B. RADIUS
- C. GRE
- D. IPSec

Answer: B

Explanation:

QUESTION NO: 1255

A webpage displays a potentially offensive advertisement on a computer. A customer walking by notices the displayed advertisement and files complaint. Which of the following can BEST reduce the likelihood of this incident occurring again?

- A. Clean-desk policies
- B. Screen-locks
- C. Pop-up blocker
- D. Antispyware software

Answer: C

Explanation:

QUESTION NO: 1256

Which of the following is an attack designed to activate based on date?

- A. Logic bomb
- B. Backdoor
- C. Trojan
- D. Rootkit

Answer: A

Explanation:

QUESTION NO: 1257

A malicious user has collected the following list of information:

192.168.1.5 OpenSSH-Server_5.8

192.168.1.7 OpenSSH-Server_5.7

192.168.1.9 OpenSSH-Server_5.7

Which of the following techniques is MOST likely to gather this type of data?

- A. Banner grabbing
- B. Port scan
- C. Host scan
- D. Ping scan

Answer: B

Explanation:

QUESTION NO: 1258

A company wants to prevent unauthorized access to its secure data center. Which of the following security controls would be MOST appropriate?

- A. Alarm to local police
- B. Camera
- C. Security guard

D. Motion detector

Answer: C

Explanation:

QUESTION NO: 1259

Company policy requires employees to change their passwords every 60 days. The security manager has verified all systems are configured to expire passwords after 60 days. Despite the policy and technical configuration, weekly password audits suggest that some employees have had the same weak passwords in place longer than 60 days. Which of the following password parameters is MOST likely misconfigured?

- A. Minimum lifetime
- B. Complexity
- C. Length
- D. Maximum lifetime

Answer: B

Explanation:

QUESTION NO: 1260

An administrator would like to utilize encryption that has comparable speed and strength to the AES cipher without using AES itself. The cipher should be able to operate in the same modes as AES and utilize the same minimum bit strength. Which of the following algorithms should the administrator select?

- A. RC4
- B. Rijndael
- C. SHA
- D. TwoFish
- E. 3DES

Answer: A

Explanation:

QUESTION NO: 1261

A security analyst has a sample of malicious software and needs to know what the sample does. The analyst runs the sample in a carefully-controlled and monitored virtual machine to observe the software's behavior. The approach of malware analysis can BEST be described as:

- A. Static testing
- B. Security control testing
- C. White box testing
- D. Sandboxing

Answer: D

Explanation:

QUESTION NO: 1262

An SSL session is taking place. After the handshake phase has been established and the cipher has been selected, which of the following are being used to secure data in transport? (Select TWO)

- A. Symmetrical encryption
- B. Ephemeral Key generation
- C. Diffie-Hellman
- D. AES
- E. RSA
- F. Asymmetrical encryption

Answer: C,E

Explanation:

QUESTION NO: 1263

Company A and Company B both supply contractual services to a fast paced and growing auto parts manufacturer with a small local Area Network (LAN) at its local site. Company A performs in-house billing and invoices services for the local auto parts manufacturer. Company B provides in-house parts and widgets services for the local auto parts manufacturers. Which of the following is the BEST method to mitigate security risk within the environment?

- A. Virtual Private Network
- B. Role-Based access
- C. Network segmentation
- D. Public Key Infrastructure

Answer: C

Explanation:

QUESTION NO: 1264

The Chief Executive Officer (CEO) Joe notices an increase in the wireless signal in this office and thanks the IT director for the increase in network speed. Upon investigation the IT department finds an access point hidden in the dropped ceiling outside of Joe's office. Which of the following types of attack is MOST likely occurring?

- A. Packet sniffing
- B. Bluesnarfing
- C. Man-in-the-middle
- D. Evil twin

Answer: D

Explanation:

QUESTION NO: 1265

A security administrator is reviewing the company's data backup plan. The plan implements nightly offsite data replication to a third party company. Which of the following documents specifies how much data can be stored offsite, and how quickly the data can be retrieved by the company from the third party?

- A. MTBF
- B. SLA
- C. RFQ
- D. ALE

Answer: B

Explanation:

QUESTION NO: 1266

Which of the following authentication services uses a default TCP port of 88?

- A. Kerberos

- B. TACACS+
- C. SAML
- D. LDAP

Answer: A

Explanation:

QUESTION NO: 1267

A technician has been tasked with installing and configuring a wireless access point for the engineering department. After the AP has been installed, there have been reports the employees from other departments have been connecting to it without approval. Which of the following would BEST address these concerns?

- A. Change the SSID of the AP so that it reflects a different department, obscuring its ownership
- B. Implement WPA2 encryption in addition to WEP to protect the data-in-transit
- C. Configure the AP to allow only to devices with pre-approved hardware addresses
- D. Lower the antenna's power so that it only covers the engineering department's offices

Answer: D

Explanation:

QUESTION NO: 1268

A company has implemented full disk encryption. Clients must authenticate with a username and password at a pre-boot level to unlock the disk and again a username and password at the network login. Which of the following are being used? (Select TWO)

- A. Multifactor authentication
- B. Single factor authentication
- C. Something a user is
- D. Something a user has
- E. Single sign-on
- F. Something a user knows

Answer: B,F

Explanation:

QUESTION NO: 1269

Anne an employee receives the following email:

From: Human Resources

To: Employee

Subject: Updated employee code of conduct

Please click on the following link: <http://external.site.com/codeofconduct.exe> to review the updated code of conduct at your earliest convenience.

After clicking the email link, her computer is compromised. Which of the following principles of social engineering was used to lure Anne into clicking the phishing link in the above email?

- A. Authority
- B. Familiarity
- C. Intimidation
- D. Urgency

Answer: B

Explanation:

QUESTION NO: 1270

During a review a company was cited for allowing requestors to approve and implement their own change request. Which of the following would resolve the issue? (Select TWO)

- A. Separation duties
- B. Mandatory access
- C. Mandatory vacations
- D. Audit logs
- E. Job Rotation
- F. Time of day restrictions

Answer: A,E

Explanation:

QUESTION NO: 1271

A security administrator wishes to protect session keys should a private key become discovered.

Which of the following should be enabled in IPSec to allow this?

- A. Perfect forward secrecy
- B. Key escrow
- C. Digital signatures
- D. CRL

Answer: B

Explanation:

QUESTION NO: 1272

A workstation is exhibiting symptoms of malware and the network security analyst has decided to remove the system from the network. This represents which of the following stages of the Incident Handling Response?

- A. Plan of action
- B. Mitigation
- C. Lesson Learned
- D. Recovery

Answer: A

Explanation:

QUESTION NO: 1273

Which of the following would provide the MOST objective results when performing penetration testing for an organization?

- A. An individual from outside the organization would be more familiar with the system
- B. AN inside support staff member would know more about how the system could be compromised
- C. An outside company would be less likely to skew the results in favor if the organization
- D. An outside support staff member would be more likely to report accurate results due to familiarity with the system

Answer: C

Explanation:

QUESTION NO: 1274

An administrator would like users to authenticate to the network using only UDP protocols. Which of the following would meet this goal?

- A. RADIUS
- B. TACACS+
- C. Kerberos
- D. 802.1x

Answer: A

Explanation:

QUESTION NO: 1275

When employing PKI to send signed and encrypted data the individual sending the data must have: (Select TWO)

- A. The receiver's private key
- B. The root certificate
- C. The sender's private key
- D. The sender's public key
- E. The receiver's public key

Answer: C,E

Explanation:

QUESTION NO: 1276

Joe a technician is tasked with finding a way to test operating system patches for a wide variety of servers before deployment to the production environment while utilizing a limited amount of hardware resources. Which of the following would provide the BEST environment for performing this testing?

- A. OS hardening
- B. Application control
- C. Virtualization
- D. Sandboxing

Answer: C

Explanation:

QUESTION NO: 1277

A custom PKI application downloads a certificate revocation list (CRL) once per day. Management requests the list be checked more frequently. Which of the following is the BEST solution?

- A. Refresh the CA public key each time a user logs in
- B. Download the CRK every 60 seconds
- C. Implement the OCSP protocol
- D. Prompt the user to trust a certificate each time it is used

Answer: C

Explanation:

QUESTION NO: 1278

A security technician wants to improve the strength of a weak key by making it more secure against brute force attacks. Which of the following would achieve this?

- A. Blowfish
- B. Key stretching
- C. Key escrow
- D. Recovery agent

Answer: A

Explanation:

QUESTION NO: 1279

Joe uses his badge to enter the server room, Ann follows Joe entering without using her badge. It is later discovered that Ann used a USB drive to remove confidential data from a server. Which of the following principles is potentially being violated? (Select TWO)

- A. Clean desk policy
- B. Least privilege
- C. Tailgating
- D. Zero-day exploits

E. Data handling

Answer: C,E

Explanation:

QUESTION NO: 1280

Ann the IT director wants to ensure that as hoc changes are not making their way to the production applications. Which of the following risk mitigation strategies should she implement in her department?

- A. Change management
- B. Permission reviews
- C. Incident management
- D. Perform routine audits

Answer: A

Explanation:

QUESTION NO: 1281

Which of the following would allow users from outside of an organization to have access to internal resources?

- A. NAC
- B. VLANS
- C. VPN
- D. NAT

Answer: C

Explanation:

QUESTION NO: 1282

Which of the following is BEST described by a scenario where management chooses not to implement a security control for a given risk?

- A. Mitigation

- B. Avoidance
- C. Acceptance
- D. Transference

Answer: C

Explanation:

QUESTION NO: 1283

Which of the following ports is used for TELNET by default?

- A. 22
- B. 23
- C. 21
- D. 20

Answer: B

Explanation:

QUESTION NO: 1284

When confidentiality is the primary concern which of the following types of encryption should be chosen?

- A. Digital Signature
- B. Symmetric
- C. Asymmetric
- D. Hashing

Answer: D

Explanation:

QUESTION NO: 1285

A Windows- based computer is infected with malware and is running too slowly to boot and run a malware scanner. Which of the following is the BEST way to run the malware scanner?

- A. Kill all system processes

- B. Enable the firewall
- C. Boot from CD/USB
- D. Disable the network connection

Answer: C

Explanation:

QUESTION NO: 1286

Ann a member of the Sales Department has been issued a company-owned laptop for use when traveling to remote sites. Which of the following would be MOST appropriate when configuring security on her laptop?

- A. Configure the laptop with a BIOS password
- B. Configure a host-based firewall on the laptop
- C. Configure the laptop as a virtual server
- D. Configure a host based IDS on the laptop

Answer: A

Explanation:

QUESTION NO: 1287

A security technician has removed the sample configuration files from a database server. Which of the following application security controls has the technician attempted?

- A. Application hardening
- B. Application baselines
- C. Application patch management
- D. Application input validation

Answer: A

Explanation:

QUESTION NO: 1288

Data confidentiality must be enforces on a secure database. Which of the following controls meets this goal? (Select TWO)

- A. MAC
- B. Lock and key
- C. Encryption
- D. Non-repudiation
- E. Hashing

Answer: C,E

Explanation:

QUESTION NO: 1289

A forensic analyst is reviewing electronic evidence after a robbery. Security cameras installed at the site do not record any footage. Which of the following types of controls was being used?

- A. Detective
- B. Corrective
- C. Deterrent
- D. Preventive

Answer: C

Explanation:

QUESTION NO: 1290

A network security administrator is trying to determine how an attacker gained access to the corporate wireless network. The network is configured with SSID broadcast disabled. The senior network administrator explains that this configuration setting would only have determined an unsophisticated attacker because of which of the following?

- A. The SSID can be obtained with a wireless packet analyzer
- B. The required information can be brute forced over time
- C. Disabling the SSID only hides the network from other WAPs
- D. The network name could be obtained through a social engineering campaign

Answer: A

Explanation:

QUESTION NO: 1291

Joe a system administrator receives reports that users attempting to reach the corporate website are arriving at an unfamiliar website instead. An investigation by a forensic analyst found that the name server log has several corporate IP addresses that were changed using Joe's credentials. Which of the following is this attack called?

- A. Xmas attack
- B. DNS poisoning
- C. Web server attack
- D. Spoofing attack

Answer: B

Explanation:

QUESTION NO: 1292

Joe a technician initiated scans if the company's 10 routers and discovered that half if the routers were not changed from their default configuration prior installed on the network. Which of the following would address this?

- A. Secure router configuration
- B. Implementing 802.1x
- C. Enabling loop protection
- D. Configuring port security

Answer: A

Explanation:

QUESTION NO: 1293

An employee attempts to go to a well-known bank site using the company-standard web browser by correctly typing in the address of the site into the web browser. The employee is directed to a website that looks like the bank's site but is not the actual bank site. The employee's user name and password are subsequently stolen. This is an example of which of the following?

- A. Watering hole attack
- B. Cross-site scripting
- C. DNS poisoning
- D. Man-in-the-middle attack

Answer: C

Explanation:

QUESTION NO: 1294

A user authenticates to a local directory server. The user then opens a virtualization client to connect to a virtual server. Instead of supplying a username/password combination, the user simply checks a use directory credentials checkbox to authenticate to the virtual server. Which of the following authentication types has been utilized?

- A. Transitive trust
- B. Common access card
- C. Multifactor authentication
- D. Single sign-on

Answer: B

Explanation:

QUESTION NO: 1295

The new Chief Information Officer (CIO) of company ABC, Joe has noticed that company XWY is always one step ahead with similar products. He tasked his Chief Security Officer to implement new security controls to ensure confidentiality of company ABC's proprietary data and complete accountability for all data transfers. Which of the following security controls did the Chief Security Officer implement to BEST meet these requirements? (Select Two)

- A. Redundancy
- B. Hashing
- C. DRP
- D. Digital Signatures
- E. Encryptions

Answer: B,E

Explanation:

QUESTION NO: 1296

A worker dressed in a fire suppression company's uniform asks to be let into the server room to perform the annual check in the fire extinguishers. The system administrator allows the worker into

the room, only to discover hours later that the worker was actually a penetration tester. Which of the following reasons allowed the penetration tester to access the server room?

- A. Testing the fire suppression system represented a critical urgency
- B. The pen tester assumed the authority of a reputable company
- C. The pen tester used an intimidation technique on the administrator
- D. The administrator trusted that the server room would remain safe

Answer: B

Explanation:

QUESTION NO: 1297

A company uses port security based on an approved MAC list to secure its wired network and WPA2 to secure its wireless network. Which of the following prevents an attacker from learning authorized MAC addresses?

- A. Port security prevents access to any traffic that might provide an attacker with authorized MAC addresses
- B. Port security uses certificates to authenticate devices and is not part of a wireless protocol
- C. Port security relies in a MAC address length that is too short to be cryptographically secure over wireless networks
- D. Port security encrypts data on the network preventing an attacker from reading authorized MAC addresses

Answer: A

Explanation:

QUESTION NO: 1298

A security technician is implementing PKI on a Network. The technician wishes to reduce the amount of bandwidth used when verifying the validity of a certificate. Which of the following should the technician implement?

- A. CSR
- B. Key escrow
- C. OSCR
- D. CRL

Answer: D

Explanation:

QUESTION NO: 1299

The network security manager has been notified by customer service that employees have been sending unencrypted confidential information via email. Which of the following should the manager select to BEST detect and provide notification of these occurrences?

- A. DLP
- B. SSL
- C. DEP
- D. UTM

Answer: A

Explanation:

QUESTION NO: 1300

While troubleshooting a new wireless 802.11 ac network an administrator discovers that several of the older systems cannot connect. Upon investigation the administrator discovers that the older devices only support 802.11 and RC4. The administrator does not want to affect the performance of the newer 802.11 ac devices on the network. Which of the following should the administrator do to accommodate all devices and provide the MOST security?

- A. Disable channel bonding to allow the legacy devices and configure WEP fallback
- B. Configure the AP in protected mode to utilize WPA2 with CCMP
- C. Create a second SSID on the AP which utilizes WPA and TKIP
- D. Configure the AP to utilize the 5Gh band only and enable WEP

Answer: B

Explanation:

QUESTION NO: 1301

A security administrator is troubleshooting an authentication issues using a network sniffer. The security administrator reviews a packet capture of the authentication process and notices that authentication is performed using extensible markup over SOAP. Which of the following authentication services is the security administrator troubleshooting?

- A. SAML
- B. XTACACS
- C. Secure LDAP
- D. RADIUS

Answer: A

Explanation:

QUESTION NO: 1302

Given a class C network a technician has been tasked with creating a separate subnet for each of the eight departments in the company. Which of the following network masks would allow for each department to have a unique network space and what is the maximum number of hosts each department could have?

- A. Network 255.255.255.192, 62 hosts
- B. Network 255.255.255.224, 30 hosts
- C. Network 255.255.255.240, 16 hosts
- D. Network 255.255.255.248, 32 hosts

Answer: D

Explanation:

QUESTION NO: 1303

A software security concern when dealing with hardware and devices that have embedded software or operating systems is:

- A. Patching may not always be possible
- B. Configuration support may not be available
- C. There is no way to verify if a patch is authorized or not
- D. The vendor may not have a method for installation of patches

Answer: D

Explanation:

QUESTION NO: 1304

A major medical corporation is investigating deploying a web based portal for patients to access

their medical records. The medical corporation has a long history of maintaining IT security but is considering having a third party vendor create the web portal. Which of the following areas is MOST important for the Chief Information Security Officer to focus on when reviewing proposal from vendors interested in creating the web portal?

- A. Contractor background check
- B. Confidentiality and availability
- C. Redundancy and privacy
- D. Integrity and confidentiality

Answer: B

Explanation:

QUESTION NO: 1305

Which of the following authentication methods requires the user, service provider and an identity provider to take part in the authentication process?

- A. RADIUS
- B. SAML
- C. Secure LDAP
- D. Kerberos

Answer: A

Explanation:

QUESTION NO: 1306

Which of the following types of malware is designed to provide access to a system when normal authentication fails?

- A. Rootkit
- B. Botnet
- C. Backdoor
- D. Adware

Answer: C

Explanation:

QUESTION NO: 1307

Ann is concerned that the application her team is currently developing is vulnerable to unexpected user input that could lead to issues within the memory is affected in a detrimental manner leading to potential exploitation. Which of the following describes this application threat?

- A. Replay attack
- B. Zero-day exploit
- C. Distributed denial of service
- D. Buffer overflow

Answer: C

Explanation:

QUESTION NO: 1308

Which of the following can be used for both encryption and digital signatures?

- A. 3DES
- B. AES
- C. RSA
- D. MD5

Answer: A

Explanation:

QUESTION NO: 1309

A user tries to visit a web site with a revoked certificate. In the background a server from the certificate authority only sends the browser revocation information about the domain the user is visiting. Which of the following is being used by the certificate authority in this exchange?

- A. CSR
- B. Key escrow
- C. OCSP
- D. CRL

Answer: D

Explanation:

QUESTION NO: 1310

Joe wants to employ MD5 hashing on the company file server. Which of the following is Joe trying to achieve?

- A. Availability
- B. Confidentiality
- C. Non repudiation
- D. Integrity

Answer: B

Explanation:

QUESTION NO: 1311

By hijacking unencrypted cookies an application allows an attacker to take over existing web sessions that do not use SSL or end to end encryption. Which of the following choices BEST mitigates the security risk of public web surfing? (Select TWO)

- A. WPA2
- B. WEP
- C. Disabling SSID broadcasting
- D. VPN
- E. Proximity to WIFI access point

Answer: C,D

Explanation:

QUESTION NO: 1312

The security administration team at a company has been tasked with implementing a data-at-rest solution for its company storage. Due to the large amount of storage the Chief Information Officer (CISO) decides that a 128-bit cipher is needed but the CISO also does not want to degrade system performance any more than necessary. Which of the following encryptions needs BOTH of these needs?

- A. SHA1
- B. DSA

- C. AES
- D. 3DES

Answer: C

Explanation:

QUESTION NO: 1313

A company has a BYOD policy that includes tablets and smart phones. In the case of a legal investigation, which of the following poses the greatest security issues?

- A. Recovering sensitive documents from a device if the owner is unable or unwilling to cooperate
- B. Making a copy of all of the files on the device and hashing them after the owner has provided the PIN
- C. Using GPS services to locate the device owner suspected in the investigation
- D. Wiping the device from a remote location should it be identified as a risk in the investigation

Answer: A

Explanation:

QUESTION NO: 1314

After several thefts a Chief Executive Officer (CEO) wants to ensure unauthorized do not have to corporate grounds or its employees. The CEO just approved new budget line items for fences, lighting, locks and CCTVs. Which of the following is the primary focus?

- A. Safety
- B. Confidentiality
- C. Availability
- D. Integrity

Answer: A

Explanation:

QUESTION NO: 1315

Which of the following steps in incident response procedures entails of the incident and identification of knowledge gained that can be applied to future handling of incidents?

- A. Recovery procedures
- B. Escalation and notification
- C. Reporting
- D. Lessons learned

Answer: D

Explanation:

QUESTION NO: 1316

Which of the following automated or semi-automated software testing techniques relies on inputting large amounts of random data to detect coding errors or application loopholes?

- A. Fuzzing
- B. Black box
- C. Fault injection
- D. SQL injection

Answer: A

Explanation:

QUESTION NO: 1317

A company's BYOD policy requires the installation of a company provide mobile agent on their on their personally owned devices which would allow auditing when an employee wants to connect a device to the corporate email system. Which of the following concerns will MOST affect the decision to use a personal device to receive company email?

- A. Personal privacy
- B. Email support
- C. Data ownership
- D. Service availability

Answer: A

Explanation:

QUESTION NO: 1318

A penetration tester is measuring a company's posture on social engineering. The penetration

tester sends a phishing email claiming to be from IT asking employees to click a link to update their VPN software immediately. Which of the following reasons would explain why this attack could be successful?

- A. Principle of Scarcity
- B. Principle of Intimidation
- C. Principle of Urgency
- D. Principle of liking

Answer: C

Explanation:

QUESTION NO: 1319

A new employee has joined the accounting department and is unable to access the accounting server. The employee can access other network resources and the Internet. Other accounting employees are able to access the accounting server without any issues. Which of the following is the MOST likely issue?

- A. The server's IDS is blocking the new employee's connection
- B. The workstation is unable to join the domain
- C. The server's drive is not mapped on the new employee's workstation
- D. The new account is not in the proper role-based profile

Answer: D

Explanation:

QUESTION NO: 1320

Joe a sales employee is connecting to a wireless network and has entered the network information correctly. His computer remains connected to the network but he cannot access any resources on the network. Which of the following is the MOST likely cause of this issue?

- A. The encryption is too strong
- B. The network SSID is disabled
- C. MAC filtering is enabled
- D. The wireless antenna power is set too low

Answer: D

Explanation:

QUESTION NO: 1321

Which of the following is used to inform users of the repercussions of releasing proprietary information?

- A. OLA
- B. SLA
- C. NDA
- D. MOU

Answer: C

Explanation:

QUESTION NO: 1322

A review of administrative access has discovered that too many accounts have been granted administrative rights. Which of the following will alert the security team when elevated access is applied?

- A. Establishing user access reviews
- B. Establishing user based privileges
- C. Establishing monitoring on accounts
- D. Establishing group based privileges

Answer: C

Explanation:

QUESTION NO: 1323

When an authorized application is installed on a server, the application triggers an alert on the HIDS. This is known as a:

- A. Vulnerability
- B. False negative
- C. False positive
- D. Threat vector

Answer: C

Explanation:

QUESTION NO: 1324

In which of the following scenarios would it be preferable to implement file level encryption instead of whole disk encryption?

- A.** A server environment where the primary security concern is integrity and not file recovery
- B.** A cloud storage environment where multiple customers use the same hardware but possess different encryption keys
- C.** A SQL environment where multiple customers access the same database
- D.** A large datacenter environment where each customer users dedicated hardware resources

Answer: B

Explanation:

QUESTION NO: 1325

For high availability which of the following would be MOST appropriate for fault tolerance?

- A.** RAID 0
- B.** Clustering
- C.** JBOD
- D.** Load Balancing

Answer: D

Explanation:

QUESTION NO: 1326

When implementing a Public Key Infrastructure, which of the following should the sender use to digitally sign a document?

- A.** A CSR
- B.** A private key
- C.** A certificate authority
- D.** A public key

Answer: B

Explanation:

QUESTION NO: 1327

A military base wants to incorporate biometrics into its new security measures, but the head of security does not want them to be the sole method of authentication. For unmanned entry points, which of the following solutions would work BEST?

- A. Use voice print and a bollard
- B. Use a retina scanner and a thumbprint
- C. Use CCTV and a PIN
- D. Use a retina scan and a PIN code

Answer: D

Explanation:

QUESTION NO: 1328

Ann a security administrator wants a limit access to the wireless network. Which of the following can be used to do this without using certificates?

- A. Employ EPA-TLS
- B. Employ PEAP on all laptops
- C. Enable MAC filtering
- D. Disable SSID broadcasting

Answer: C

Explanation:

QUESTION NO: 1329

A user has an Android smartphone that supports full device encryption. However when the user plug into a computer all of the files are immediately accessible. Which of the following should the user do to enforce full device confidentiality should the phone be lost or stolen?

- A. Establish a PIN passphrase
- B. Agree to remote wipe terms

- C. Generate new media encryption keys
- D. Download the encryption control app from the store

Answer: A

Explanation:

QUESTION NO: 1330

The network manager has obtained a public IP address for use with a new system to be available via the internet. This system will be placed in the DMZ and will communicate with a database server on the LAN. Which of the following should be used to allow for proper communication between internet users and the internal systems?

- A. VLAN
- B. DNS
- C. NAT
- D. HTTP
- E. SSL

Answer: E

Explanation:

QUESTION NO: 1331

After a new RADIUS server is added to the network, an employee is unable to connect to the company's WPA2-Enterprise WIFI network, which is configured to prompt for the employee's network username and password. The employee reports receiving an error message after a brief connection attempt, but is never prompted for credentials. Which of the following issues could be causing the problem?

- A. The employee's account is locked out in the directory service
- B. The new RADIUS server is overloading the wireless access point
- C. The new RADIUS server's certificate is not trusted by the employee's PC
- D. The employee's account is disabled in the RADIUS server's local database

Answer: A

Explanation:

QUESTION NO: 1332

Ann the security administrator has been reviewing logs and has found several overnight sales personnel are accessing the finance department's network shares. Which of the following security controls should be implemented to BEST remediate this?

- A. Mandatory access
- B. Separation of duties
- C. Time of day restrictions
- D. Role based access

Answer: C

Explanation:

QUESTION NO: 1333

A fiber company has acquired permission to bury a fiber cable through a farmer's land. Which of the following should be in the agreement with the farmer to protect the availability of the network?

- A. No farm animals will graze near the burial site of the cable
- B. No digging will occur near the burial site of the cable
- C. No buildings or structures will be placed on top of the cable
- D. No crops will be planted on top of the cable

Answer: B

Explanation:

QUESTION NO: 1334

The programmer confirms that there is potential for a buffer overflow on one of the data input fields in a corporate application. The security analyst classifies this as a (N).

- A. Threat
- B. Risk
- C. Attack
- D. Vulnerability

Answer: D

Explanation:

QUESTION NO: 1335

A security technician would like to use ciphers that generate ephemeral keys for secure communication. Which of the following algorithms support ephemeral modes? (Select TWO)

- A. Diffie-Hellman
- B. RC4
- C. RIPEMO
- D. NTLMv2
- E. PAP
- F. RSA

Answer: A,F

Explanation:

QUESTION NO: 1336

A security technician would like an application to use random salts to generate short lived encryption keys during the secure communication handshake process to increase communication security. Which of the following concepts would BEST meet this goal?

- A. Ephemeral keys
- B. Symmetric Encryption Keys
- C. AES Encryption Keys
- D. Key Escrow

Answer: B

Explanation:

QUESTION NO: 1337

A security administrator wishes to implement a method of generating encryption keys from user passwords to enhance account security. Which of the following would accomplish this task?

- A. NTLMv2
- B. Blowfish
- C. Diffie-Hellman
- D. PBKDF2

Answer: C

Explanation:

QUESTION NO: 1338

An administrator needs to allow both secure and regular web traffic into a network. Which of the following ports should be configured? (Select TWO)

- A. 25
- B. 53
- C. 80
- D. 110
- E. 143
- F. 443

Answer: C,F

Explanation:

QUESTION NO: 1339

A recent audit had revealed weaknesses in the process of deploying new servers and network devices. Which of the following practices could be used to increase the security posture during deployment? (Select TWO).

- A. Deploy a honeypot
- B. Disable unnecessary services
- C. Change default password
- D. Implement an application firewall
- E. Penetration testing

Answer: B,C

Explanation:

QUESTION NO: 1340

A local hospital with a large four-acre campus wants to implement a wireless network so that doctors can use tablets to access patients' medical data. The hospital also wants to provide guest access to the internet for hospital patients and visitors in select areas. Which of the following areas

should be addressed FIRST?

- A. MAC filters
- B. Site Survey
- C. Power level controls
- D. Antenna types

Answer: B

Explanation:

QUESTION NO: 1341

After making a bit-level copy of compromised server, the forensics analyst Joe wants to verify that he did not accidentally make a change during his investigation. Which of the following should he perform?

- A. Take a hash of the image and compare it to the one being investigated
- B. Compare file sizes of all files prior to and after investigation
- C. Make a third image and compare it to the second image being investigated
- D. Compare the logs of the copy to the actual server

Answer: A

Explanation:

QUESTION NO: 1342

Which of the following attacks is generally initiated from a botnet?

- A. Cross site scripting attack
- B. HTTP header injection
- C. Distributed denial of service
- D. A war driving attack

Answer: C

Explanation:

QUESTION NO: 1343

A network security analyst has confirmed that the public facing web server has been compromised. Which of the following stages if the Incident Handling Response does this describe?

- A. Analyzing
- B. Recovering
- C. Identification
- D. Mitigation

Answer: C

Explanation:

QUESTION NO: 1344

Deploying compensating security controls is an example of:

- A. Risk avoidance
- B. Risk mitigation
- C. Risk transference
- D. Risk acceptance

Answer: B

Explanation:

QUESTION NO: 1345

A web startup wants to implement single sign-on where its customers can log on to the site by suing their personal and existing corporate email credentials regardless of which company they work for. Is this directly supported by SAML?

- A. Mo not without extensive partnering and API integration with all required email providers
- B. Yes SAML is a web based single sign-on implementation exactly fir this purpose
- C. No a better approach would be to use required email providers LDAP or RADIUS repositories
- D. Yes SAML can use oauth2 to provide this functionality out of the box

Answer: A

Explanation:

QUESTION NO: 1346

A security administrator is installing a single camera outside in order to detect unauthorized vehicles in the parking lot. Which of the following is the MOST important consideration when deploying a CCTV camera to meet the requirement?

- A. Training
- B. Expense
- C. Resolution
- D. Field of view

Answer: C

Explanation:

QUESTION NO: 1347

A system administrator wants to configure a setting that will make offline password cracking more challenging. Currently the password policy allows upper and lower case characters a minimum length of 5 and a lockout after 10 invalid attempts. Which of the following has the GREATEST impact on the time it takes to crack the passwords?

- A. Increase the minimum password length to 8 while keeping the same character set
- B. Implement an additional password history and reuse policy
- C. Allow numbers and special characters in the password while keeping the minimum length at 5
- D. Implement an account lockout policy after three unsuccessful logon attempts

Answer: D

Explanation:

QUESTION NO: 1348

Establishing a method to erase or clear memory is an example of securing which of the following?

- A. Data in transit
- B. Data at rest
- C. Data in use
- D. Data in motion

Answer: B

Explanation:

QUESTION NO: 1349

Joe processes several requisitions during the day and during the night shift they are approved by Ann. This is an example of which of the following?

- A. Separation of duties
- B. Discretionary access
- C. Mandatory access
- D. Time of day restrictions

Answer: B

Explanation:

QUESTION NO: 1350

A security administrator would like to write an access rule to block the three IP addresses given below. Which of the following combinations should be used to include all of the given IP addresses?

192.168.12.255

192.168.12.227

192.168.12.229

- A. 192.168.12.0/25
- B. 192.168.12.128.28
- C. 192.168.12.224/29
- D. 192.168.12.225/30

Answer: B

Explanation:

QUESTION NO: 1351

After installing a new Linux system the administrator runs a command that records the size, permissions, and MD5 sum of all the files on the system. Which of the following describes what the administrator is doing?

- A. Identifying vulnerabilities
- B. Design review
- C. Host software baselining
- D. Operating system hardening

Answer: C

Explanation:

QUESTION NO: 1352

An intrusion has occurred in an internet facing system. The security administrator would like to gather forensic evidence while the system is still in operation. Which of the following procedures should the administrator perform FIRST on the system?

- A. Make a drive image
- B. Take hashes of system data
- C. Collect information in RAM
- D. Capture network traffic

Answer: D

Explanation:

QUESTION NO: 1353

Which of the following wireless standards is backwards compatible with 802.11g?

- A. 802.11a
- B. 802.11b
- C. 802.11n
- D. 802.1q

Answer: B

Explanation:

QUESTION NO: 1354

Which of the following ports will be used for logging into secure websites?

- A. 80
- B. 110
- C. 142
- D. 443

Answer: D

Explanation:

QUESTION NO: 1355

The below report indicates that the system is MOST likely infected by which of the following?

Protocol LOCAL IP FOREIGN IP STATE

TCP 0.0.0:445 0.0.0.0:0 Listening

TCP 0.0.0.0:3390 0.0.0.0:0 Listening

- A. Trojan
- B. Worm
- C. Logic bomb
- D. Spyware

Answer: A

Explanation:

QUESTION NO: 1356

A security administrator is required to submit a detailed implementation plan and back out plan to get approval prior to updating the firewall and other security devices. Which of the following types of risk mitigation strategies is being followed?

- A. Change management
- B. Routine audit
- C. Rights and permissions review
- D. Configuration management

Answer: D

Explanation:

QUESTION NO: 1357

Which of the following authentication services uses a default TCP of 389?

- A. SAML
- B. TACACS+
- C. Kerberos
- D. LDAP

Answer: D

Explanation:

QUESTION NO: 1358

A software company sends their offsite backup tapes to a third party storage facility. TO meet confidentiality the tapes should be:

- A. Labeled
- B. Hashed
- C. Encrypted
- D. Duplicated

Answer: A

Explanation:

QUESTION NO: 1359

Ann, a technician, wants to implement a single protocol on a remote server which will enable her to encrypt and proxy all of her traffic though the remote server via SOCKS5. Which of the following should Ann enable to support both encryption and proxy services?

- A. SSH
- B. IPSEC
- C. TLS
- D. HTTPS

Answer: A

Explanation:

QUESTION NO: 1360

Ann, a system analyst, discovered the following log. Which of the following techniques does this indicate?

```
{bp1@localmachine}$ ls-al
```

Total 12

```
Drwxrwxr-x
```

```
drwxrwxr-x.  2 bp1 businesspartner 4096 Apr 18 05:19 .
drwx----- 22 bp1 businesspartner 4096 Apr 19 05:19 ..
-rw-rw-r--.  1 bp1 businesspartner 5023801 Apr 19 05:19 businesspartnerstatements18-4.csv
-rw-rw-r--.  1 bp1 businesspartner 7812851 Apr 20 05:19 businesspartnerstatements17-4.bt
-rw-rw-r--.  1 bp1 businesspartner 1739017 Apr 21 05:19 businesspartnerstatements16-4.csv
[nessus log] evil user sftp * 139.130.4.5: businesspartnerstatements18-4.csv
[nessus log] evil user sftp * 139.130.4.5: businesspartnerstatements18-4.csv
```

- A. Protocol analyzer
- B. Port scanner
- C. Vulnerability
- D. Banner grabbing

Answer: A

Explanation:

QUESTION NO: 1361

A company discovers an unauthorized device accessing network resources through one of many network drops in a common area used by visitors. The company decides that it wants to quickly prevent unauthorized devices from accessing the network but policy prevents the company from making changes on every connecting client. Which of the following should the company implement?

- A. Port security
- B. WPA2
- C. Mandatory Access Control
- D. Network Intrusion Prevention

Answer: A

Explanation:

QUESTION NO: 1362

The helpdesk is receiving numerous reports that a newly installed biometric reader at the entrance of the data center has a high of false negatives. Which of the following is the consequence of this reported problem?

- A. Unauthorized employees have access to sensitive systems
- B. All employees will have access to sensitive systems
- C. No employees will be able to access the datacenter
- D. Authorized employees cannot access sensitive systems

Answer: C

Explanation:

QUESTION NO: 1363

A software developer places a copy of the source code for a sensitive internal application on a company laptop to work remotely. Which of the following policies is MOST likely being violated?

- A. Clean desk
- B. Data handling
- C. Chain of custody
- D. Social media

Answer: B

Explanation:

QUESTION NO: 1364

While testing a new host based firewall configuration a security administrator inadvertently blocks access to localhost which causes problems with applications running on the host. Which of the following addresses refer to localhost?

- A. ::0
- B. 127.0.0.0
- C. 120.0.0.1
- D. 127.0.0/8
- E. 127::0.1

Answer: C

Explanation:

QUESTION NO: 1365

A user has reported inadvertently sending an encrypted email containing PII to an incorrect distribution group. Which of the following potential incident types is this?

- A. Data sharing
- B. Unauthorized viewing
- C. Data breach
- D. Unauthorized access

Answer: B

Explanation:

QUESTION NO: 1366

A company is exploring the option of letting employees use their personal laptops on the internal network. Which of the following would be the MOST common security concern in this scenario?

- A. Credential management
- B. Support ownership
- C. Device access control
- D. Antivirus management

Answer: D

Explanation:

QUESTION NO: 1367

A security engineer discovers that during certain times of day, the corporate wireless network is dropping enough packets to significantly degrade service. Which of the following should be the engineer's FIRST step in troubleshooting the issues?

- A. Configure stronger encryption
- B. Increase the power level
- C. Change to a higher gain antenna
- D. Perform a site survey

Answer: B

Explanation:

QUESTION NO: 1368

A security administrator is reviewing the web logs and notices multiple attempts by users to access: http://www.comptia.org/idapsearch?user-*

Having identified the attack, which of the following will prevent this type of attack on the web server?

- A. Input validation on the web server
- B. Block port 389 on the firewall
- C. Segregate the web server by a VLAN
- D. Block port 3389 on the firewall

Answer: A

Explanation:

QUESTION NO: 1369

A breach at a credit card company resulted in customers credit card information being exposed . The company has conducted a full forensic investigation and identified the source of the breach. Which of the following should the company do NEXT?

- A. Move to the incident identification phase
- B. Implement the risk assessment plan
- C. Implement damage and loss control procedures
- D. Implement first responder processes

Answer: C

Explanation:

QUESTION NO: 1370

Joe a user upon arriving to work on Monday morning noticed several files were deleted from the system. There were no records of any scheduled network outages or upgrades to the system. Joe notifies the security department of the anomaly found and removes the system from the network.

Which of the following is the NEXT action that Joe should perform?

- A. Screenshots of systems
- B. Call the local police
- C. Perform a backup
- D. Capture system image

Answer: A

Explanation:

QUESTION NO: 1371

The user of a news service accidentally accesses another user's browsing history. From this the user can tell what competitors are reading, querying, and researching. The news service has failed to properly implement which of the following?

- A. Application white listing
- B. In-transit protection
- C. Access controls
- D. Full disk encryption

Answer: C

Explanation:

QUESTION NO: 1372

A system requires administrators to be logged in as the "root" in order to make administrator changes. Which of the following controls BEST mitigates the risk associated with this scenario?

- A. Require that all administrators keep a log book of times and justification for accessing root
- B. Encrypt all users home directories using file-level encryption
- C. Implement a more restrictive password rotation policy for the shared root account
- D. Force administrator to log in with individual accounts and switch to root
- E. Add the administrator to the local group

Answer: D

Explanation:

QUESTION NO: 1373

A defense contractor wants to use one of its classified systems to support programs from multiple intelligence agencies. Which of the following **MUST** be in place between the intelligence agencies to allow this?

- A. A DRP
- B. An SLA
- C. A MOU
- D. A BCP

Answer: C

Explanation:

QUESTION NO: 1374

A penetration tester was able to obtain elevated privileges on a client workstation and multiple servers using the credentials of an employee. Which of the following controls would mitigate these issues? (Select TWO)

- A. Separation of duties
- B. Least privilege
- C. Time of day restrictions
- D. Account expiration
- E. Discretionary access control
- F. Password history

Answer: B,D

Explanation:

QUESTION NO: 1375

Which of the following is considered the **MOST** effective practice when securing printers or scanners in an enterprise environment?

- A. Routine vulnerability scanning of peripherals
- B. Install in a hardened network segment
- C. Turn off the power to the peripherals at night
- D. Enable print sharing only from workstations

Answer: A

Explanation:**QUESTION NO: 1376**

After a few users report problems with the wireless network, a system administrator notices that a new wireless access point has been powered up in the cafeteria. The access point has the same SSID as the corporate network and is set to the same channel as nearby access points. However, the AP has not been connected to the Ethernet network. Which of the following is the MOST likely cause of the user's wireless problems?

- A. AP channel bonding
- B. An evil twin attack
- C. Wireless interference
- D. A rogue access point

Answer: B

Explanation:**QUESTION NO: 1377**

A network technician at a company, Joe is working on a network device. He creates a rule to prevent users from connecting to a toy website during the holiday shopping season. This website is blacklisted and is known to have SQL injections and malware. Which of the following has been implemented?

- A. Mandatory access
- B. Network separation
- C. Firewall rules
- D. Implicit Deny

Answer: D

Explanation:**QUESTION NO: 1378**

Company XYZ has suffered leaks of internally distributed confidential documents. Ann the network security analyst has been tasked to track down the culprit. She has decided to embed a four letter string of characters in documents containing proprietary information. Which of the following initial

steps should Ann implement before sending documents?

- A. Store one of the documents in a honey pot
- B. Start antivirus scan on all the suspected computers
- C. Add a signature to the NIDS containing the four letter string
- D. Ask employees to report suspicious behaviors

Answer: C

Explanation:

QUESTION NO: 1379

Which of the following should a company deploy to prevent the execution of some types of malicious code?

- A. Least privilege accounts
- B. Host-based firewalls
- C. Intrusion Detection systems
- D. Application white listing

Answer: B

Explanation:

QUESTION NO: 1380

An administrator is investigating a system that may potentially be compromised and sees the following log entries on the router.

*Jul 15 14:47:29.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 3 packets.

*Jul 15 14:47:38.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 6 packets.

*Jul 15 14:47:45.779: %Router1: list 101 permitted TCP 192.10.3.204(57222) (FastEthernet 0/3) -> 10.10.1.5 (6667), 8 packets.

Which of the following BEST describes the compromised system?

- A. It is running a rogue web server

- B. It is being used in a man-in-the-middle attack
- C. It is participating in a botnet
- D. It is an ARP poisoning attack

Answer: C

Explanation:

QUESTION NO: 1381

A security administrator implements a web server that utilizes an algorithm that requires other hashing standards to provide data integrity. Which of the following algorithms would meet the requirement?

- A. SHA
- B. MD5
- C. RIPEMD
- D. HMAC

Answer: A

Explanation:

QUESTION NO: 1382

Which of the following is the FIRST step in a forensics investigation when a breach of a client's workstation has been confirmed?

- A. Transport the workstation to a secure facility
- B. Analyze the contents of the hard drive
- C. Restore any deleted files and / or folders
- D. Make a bit-for-bit copy of the system

Answer: D

Explanation:

QUESTION NO: 1383

Company XYZ's laptops was recently stolen from a user which led to the exposure of confidential information. Which of the following should the security team implement on laptops to prevent future compromise?

- A. Cipher locks
- B. Strong passwords
- C. Biometrics
- D. Full Disk Encryption

Answer: D

Explanation:

QUESTION NO: 1384

A wireless site survey has been performed at a company. One of the results of the report is that the wireless signal extends too far outside the building. Which of the following security issues could occur as a result of this finding?

- A. Excessive wireless access coverage
- B. Interference with nearby access points
- C. Exhaustion of DHCP address pool
- D. Unauthorized wireless access

Answer: D

Explanation:

QUESTION NO: 1385

Which of the following is a software vulnerability that can be avoided by using input validation?

- A. Buffer overflow
- B. Application fuzzing
- C. Incorrect input
- D. Error handling

Answer: C

Explanation:

QUESTION NO: 1386

A university has a building that holds the power generators for the entire campus. A risk assessment was completed for the university and the generator building was labeled as a high risk. Fencing and lighting was installed to reduce risk. Which of the following security goals would

this meet?

- A. Load balancing
- B. Non-repudiation
- C. Disaster recovery
- D. Physical security

Answer: D

Explanation:

QUESTION NO: 1387

Log file analysis on a router reveals several unsuccessful telnet attempts to the virtual terminal (VTY) lines. Which of the following represents the BEST configuration used in order to prevent unauthorized remote access while maintaining secure availability for legitimate users?

- A. Disable telnet access to the VTY lines, enable SSH access to the VTY lines with RSA encryption
- B. Disable both telnet and SSH access to the VTY lines, requiring users to log in using HTTP
- C. Disable telnet access to the VTY lines, enable SSH access to the VTY lines with PSK encryption
- D. Disable telnet access to the VTY lines, enable SSL access to the VTY lines with RSA encryption

Answer: C

Explanation:

QUESTION NO: 1388

Four weeks ago a network administrator applied a new IDS and allowed it to gather baseline data. As rumors of a layoff begins to spread, the IDS alerted the network administrator that access to sensitive client files had risen for above normal. Which of the following kind of IDS is in use?

- A. Protocol based
- B. Heuristic based
- C. Signature based
- D. Anomaly based

Answer: D

Explanation:

QUESTION NO: 1389

A BYOD policy in which employees are able to access the wireless guest network is in effect in an organization. Some users however are using the Ethernet port in personal laptops to the wired network. Which of the following could an administrator use to ensure that unauthorized devices are not allowed to access the wired network?

- A. VLAN access rules configured to reject packets originating from unauthorized devices
- B. Router access lists configured to block the IP addresses of unauthorized devices
- C. Firewall rules configured to block the MAC addresses of unauthorized devices
- D. Port security configured shut down the port when unauthorized devices connect

Answer: D

Explanation:

QUESTION NO: 1390

During an office move a sever containing the employee information database will be shut down and transported to a new location. Which of the following would BEST ensure the availability of the employee database should happen to the server during the move?

- A. The contents of the database should be encrypted; the encryption key should be stored off-site
- B. A hash of the database should be taken and stored on an external drive prior to the move
- C. The database should be placed on a drive that consists of a RAID array prior to the move
- D. A backup of the database should be stored on an external hard drive prior to the move

Answer: D

Explanation:

QUESTION NO: 1391

Which of the following is primarily used to provide fault tolerance at the application level? (Select TWO)

- A. Load balancing
- B. RAID array
- C. RAID 6

- D. Server clustering
- E. JBOD array

Answer: B,D

Explanation:

QUESTION NO: 1392

A security administrator would like the corporate webserver to select perfect forward secrecy ciphers first. Which of the following cipher suites should the administrator select to accomplish this goal?

- A. DH-DSS-CAMELLA256-SHA
- B. ECDHE-RSA-AES1280SHA
- C. DH-RSA-AES128-SHA256
- D. ADH-AES256-SHA

Answer: B

Explanation:

QUESTION NO: 1393

An administrator is having difficulty configuring WPA2 Enterprise using EAP-PEAP-MSCHAPv2. The administrator has configured the wireless access points properly, and has configured policies on the RADIUS server and configured settings on the client computers. Which of the following is missing?

- A. Client certificates are needed
- B. A third party LEAP client must be installed
- C. A RADIUS server certificate is needed
- D. The use of CCMP rather than TKIP

Answer: A

Explanation:

QUESTION NO: 1394

A business has recently adopted a policy allowing employees to use personal cell phones and tablets to access company email accounts while out of the office. Joe an employee was using a

personal cell phone for email access and was recently terminated. It is suspected that Joe saved confidential client emails on his personal cell phone. Joe claims that the data on the phone is completely personal and refuse to allow the company access to inspect the cell phone. Which of the following is the MOST likely cause of this dispute?

- A. Onboarding procedures
- B. Fair use policy
- C. Device ownership
- D. User acceptance

Answer: C

Explanation:

QUESTION NO: 1395

Mobile tablets are used by employees on the sales floor to access customer data. Ann a customer recently reported that another customer was able to access her personal information on the tablet after the employee left the area. Which of the following would BEST prevent these issues from reoccurring?

- A. Screen Locks
- B. Full-device encryption
- C. Application control
- D. Asset tracking

Answer: A

Explanation:

QUESTION NO: 1396

Which of the following metrics is important for measuring the extent of data required during backup and recovery?

- A. MOU
- B. ARO
- C. ALE
- D. RPO

Answer: C

Explanation:

QUESTION NO: 1397

Which of the following can be used to ensure that sensitive records stored on a backend server can only be accessed by a front end server with the appropriate record key?

- A. File encryption
- B. Storage encryption
- C. Database encryption
- D. Full disk encryption

Answer: A

Explanation:

QUESTION NO: 1398

Which of the following would be used to allow a subset of traffic from a wireless network to an internal network?

- A. Access control list
- B. 802.1X
- C. Port security
- D. Load balancers

Answer: B

Explanation:

QUESTION NO: 1399

A company has identified a watering hole attack. Which of the following Best describes this type of attack?

- A. Emails are being spoofed to look like they are internal emails
- B. A cloud storage site is attempting to harvest user IDS and passwords
- C. An online news site is hosting ads in iframes from another site
- D. A local restaurant chains online menu is hosting malicious code

Answer: C

Explanation:

QUESTION NO: 1400

A security manager is discussing change in the security posture of the network, if a proposed application is approved for deployment. Which of the following is the MOST important the security manager must rely upon to help make this determination?

- A. Ports used by new application
- B. Protocols/services used by new application
- C. Approved configuration items
- D. Current baseline configuration

Answer: B

Explanation:

QUESTION NO: 1401

Joe the system administrator has noticed an increase in network activity from outside sources. He wishes to direct traffic to avoid possible penetration while heavily monitoring the traffic with little to no impact on the current server load. Which of the following would be BEST course of action?

- A. Apply an additional firewall ruleset on the user PCs.
- B. Configure several servers into a honeynet
- C. Implement an IDS to protect against intrusion
- D. Enable DNS logging to capture abnormal traffic

Answer: B

Explanation:

QUESTION NO: 1402

An assessment too reports that the company's web server may be susceptible to remote buffer overflow. The web server administrator insists that the finding is a false positive. Which of the following should the administrator do to verify if this is indeed a false positive?

- A. Use a banner grabbing tool
- B. Run a vulnerability scan

- C. Enforce company policies
- D. Perform a penetration test

Answer: B

Explanation:

QUESTION NO: 1403

The sales force in an organization frequently travel to remote sites and requires secure access to an internal server with an IP address of 192.168.0.220. Assuming services are using default ports, which of the following firewall rules would accomplish this objective? (Select Two)

- A. Permit TCP 20 any 192.168.0.200
- B. Permit TCP 21 any 192.168.0.200
- C. Permit TCP 22 any 192.168.0.200
- D. Permit TCP 110 any 192.168.0.200
- E. Permit TCP 139 any 192.168.0.200
- F. Permit TCP 3389 any 192.168.0.200

Answer: C,F

Explanation:

QUESTION NO: 1404

Ann, a security administrator at a call center, has been experiencing problems with users intentionally installing unapproved and occasionally malicious software on their computers. Due to the nature of their jobs, Ann cannot change their permissions. Which of the following would BEST alleviate her concerns?

- A. Deploy a HIDS suite on the users' computer to prevent application installation
- B. Maintain the baseline posture at the highest OS patch level
- C. Enable the pop-up blockers on the user's browsers to prevent malware
- D. Create an approved application list and block anything not on it

Answer: D

Explanation:

QUESTION NO: 1405

Which of the following will provide data encryption, key management and secure application launching?

- A. TKIP
- B. HSM
- C. EFS
- D. DLP

Answer: D

Explanation:

QUESTION NO: 1406

It is MOST difficult to harden against which of the following?

- A. XSS
- B. Zero-day
- C. Buffer overflow
- D. DoS

Answer: C

Explanation:

QUESTION NO: 1407

A company has experienced problems with their ISP, which has failed to meet their informally agreed upon level of service. However the business has not negotiated any additional formal agreements beyond the standard customer terms. Which of the following is the BEST document that the company should prepare to negotiate with the ISP?

- A. ISA
- B. SLA
- C. MOU
- D. PBA

Answer: B

Explanation:

QUESTION NO: 1408

A company would like to implement two-factor authentication for its vulnerability management database to require system administrators to use their token and random PIN codes. Which of the following authentication services accomplishes this objective?

- A. SAML
- B. TACACS+
- C. Kerberos
- D. RADIUS

Answer: D

Explanation:

QUESTION NO: 1409

A company has a corporate infrastructure where end users manage their own certificate keys. Which of the following is considered the MOST secure way to handle master keys associated with these certificates?

- A. Key escrow with key recovery
- B. Trusted first party
- C. Personal Identity Verification
- D. Trusted third party

Answer: A

Explanation:

QUESTION NO: 1410

A recent audit has revealed that several users have retained permissions to systems they should no longer have rights to after being promoted or changed job positions. Which of the following controls would BEST mitigate this issue?

- A. Separation of duties
- B. User account reviews
- C. Group based privileges
- D. Acceptable use policies

Answer: A

Explanation:**QUESTION NO: 1411**

Ann a new security specialist is attempting to access the internet using the company's open wireless network. The wireless network is not encrypted: however, once associated, ANN cannot access the internet or other company resources. In an attempt to troubleshoot, she scans the wireless network with NMAP, discovering the only other device on the wireless network is a firewall. Which of the following BEST describes the company's wireless network solution?

- A. The company uses VPN to authenticate and encrypt wireless connections and traffic
- B. The company's wireless access point is being spoofed
- C. The company's wireless network is unprotected and should be configured with WPA2
- D. The company is only using wireless for internet traffic so it does not need additional encryption

Answer: A

Explanation:**QUESTION NO: 1412**

Which of the following, if implemented, would improve security of remote users by reducing vulnerabilities associated with data-in-transit?

- A. Full-disk encryption
- B. A virtual private network
- C. A thin-client approach
- D. Remote wipe capability

Answer: B

Explanation:**QUESTION NO: 1413**

A company wants to improve its overall security posture by deploying environmental controls in its datacenter. Which of the following is considered an environmental control that can be deployed to meet this goal?

- A. Full-disk encryption

- B. Proximity readers
- C. Hard ward locks
- D. Fire suppression

Answer: B

Explanation:

QUESTION NO: 1414

A programmer must write a piece of code to encrypt passwords and credit card information used by an online shopping cart. The passwords must be stored using one-way encryption, while credit card information must be stored using reversible encryption. Which of the following should be used to accomplish this task? (Select TWO)

- A. SHA for passwords
- B. 3DES for passwords
- C. RC4 for passwords
- D. AES for credit cards
- E. MD5 for credit cards
- F. HMAC for credit cards

Answer: B,D

Explanation:

QUESTION NO: 1415

A company needs to provide a secure backup mechanism for key storage in a PKI. Which of the following should the company implement?

- A. Ephemeral keys
- B. Steganography
- C. Key escrow
- D. Digital signatures

Answer: C

Explanation:

QUESTION NO: 1416

A security analyst must ensure that the company's web server will not negotiate weak ciphers with connecting web browsers. Which of the following supported list of ciphers **MUST** the security analyst disable? (Select THREE)

- A. SHA
- B. AES
- C. RIPMED
- D. NULL
- E. DES
- F. MD5
- G. TWOFISH

Answer: A,E,F

Explanation:

QUESTION NO: 1417

A company's application is hosted at a data center. The data center provides security controls for the infrastructure. The data center provides a report identifying several vulnerabilities regarding out of date OS patches. The company recommends the data center assumes the risk associated with the OS vulnerabilities. Which of the following concepts is being implemented?

- A. Risk Transference
- B. Risk Acceptance
- C. Risk Avoidance
- D. Risk Deterrence

Answer: A

Explanation:

QUESTION NO: 1418

Which of the following cryptographic methods is most secure for a wireless access point?

- A. WPA with LEAP
- B. TKIP
- C. WEP with PSK
- D. WPA2 with PSK

Answer: D

Explanation:

QUESTION NO: 1419

Which of the following is considered an environmental control?

- A. Video surveillance
- B. Proper lighting
- C. EMI shielding
- D. Fencing

Answer: C

Explanation:

QUESTION NO: 1420

An attacker Joe configures his service identifier to be the same as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following Best describes this type of attack?

- A. Bluejacking
- B. WPS attack
- C. Evil twin
- D. War driving
- E. Relay attack

Answer: C

Explanation:

QUESTION NO: 1421

A company used a partner company to develop critical components of an application. Several employees of the partner company have been arrested for cybercrime activities. Which of the following should be done to protect the interest of the company?

- A. Perform a penetration test against the application
- B. Conduct a source code review of the application

- C. Perform a baseline review of the application
- D. Scan the application with antivirus and anti-spyware products.

Answer: A

Explanation:

QUESTION NO: 1422

Which of the following is a black box testing methodology?

- A. Code, function, and statement coverage review
- B. Architecture and design review
- C. Application hardening
- D. Penetration testing

Answer: A

Explanation:

QUESTION NO: 1423

A security administrator wishes to prevent certain company devices from using specific access points, while still allowing them on others. All of the access points use the same SSID and wireless password. Which of the following would be MOST appropriate in this scenario?

- A. Require clients to use 802.1x with EAPOL in order to restrict access
- B. Implement a MAC filter on the desired access points
- C. Upgrade the access points to WPA2 encryption
- D. Use low range antennas on the access points that need to be restricted

Answer: B

Explanation:

QUESTION NO: 1424

An attacker Joe configures his service identifier to be as an access point advertised on a billboard. Joe then conducts a denial of service attack against the legitimate AP causing users to drop their connections and then reconnect to Joe's system with the same SSID. Which of the following BEST describes this attack?

- A. Bluejacking
- B. WPS attack
- C. Evil twin
- D. War driving
- E. Replay attack

Answer: C

Explanation:

QUESTION NO: 1425

Which of the following may be used with a BNC connector?

- A. 10GBaseT
- B. 1000BaseSX
- C. 100BaseFX
- D. 10Base2

Answer: D

Explanation:

QUESTION NO: 1426

A network technician has received comments from several users that cannot reach a particular website. Which of the following commands would provide the BEST information about the path taken across the network to this website?

- A. Ping
- B. Netstat
- C. telnet
- D. tracer

Answer: D

Explanation:

QUESTION NO: 1427

A technician is configuring a switch to support VOIP phones. The technician wants to ensure the phones do not require external power packs. Which of the following would allow the phones to be

powered using the network connection?

- A. PoE+
- B. PBX
- C. PSTN
- D. POTS

Answer: A

Explanation:

QUESTION NO: 1428

A technician reports a suspicious individual is seen walking around the corporate campus. The individual is holding a smartphone and pointing a small antenna, in order to collect SSIDs. Which of the following attacks is occurring?

- A. Rogue AP
- B. Evil Twin
- C. Man-in-the-middle
- D. War driving

Answer: D

Explanation:

QUESTION NO: 1429

Users have reported receiving unsolicited emails in their inboxes, often times with malicious links embedded. Which of the following should be implemented in order to redirect these messages?

- A. Proxy server
- B. Spam filter
- C. Network firewall
- D. Application firewall.

Answer: B

Explanation:

QUESTION NO: 1430

A company uses SSH to support internal users. They want to block external SSH connections from reaching internal machines. Which of the following should be blocked on the firewall?

- A. 22
- B. 23
- C. 443
- D. 8080

Answer: A

Explanation:

QUESTION NO: 1431

If an organization wants to implement a BYOD policy, which of the following administrative control policy considerations **MUST** be addressed? (Select two)

- A. Data archiving
- B. Data ownership
- C. Geo-tagging
- D. Acceptable use
- E. Remote wipe

Answer: B,C

Explanation:

QUESTION NO: 1432

A security technician wants to implement stringent security controls over web traffic by restricting the client source TCP ports allowed through the corporate firewall. Which of the following should the technician implement?

- A. Deny port 80 and 443 but allow proxies
- B. Only allow port 80 and 443
- C. Only allow ports above 1024
- D. Deny ports 80 and allow port 443

Answer: B

Explanation:

QUESTION NO: 1433

An administrator is configuring a network for all users in a single building. Which of the following design elements would be used to segment the network based on organizational groups? (Select two)

- A. NAC
- B. NAT
- C. Subnetting
- D. VLAN
- E. DMZ
- F. VPN

Answer: B,C

Explanation:

QUESTION NO: 1434

A datacenter has suffered repeated burglaries which led to equipment theft and arson. In the past, the thieves have demonstrated a determination to bypass any installed safeguards. After mantraps were installed to prevent tailgating, the thieves crashed through the wall of datacenter with a vehicle after normal business hours. Which of the following options could improve the safety and security of the datacenter further? (Select two)

- A. Cipher locks
- B. CCTV
- C. Escape routes
- D. K rated fencing
- E. Fm200 fire suppression

Answer: A,D

Explanation:

QUESTION NO: 1435

Which of the following can take advantage of man in the middle techniques to prevent data exfiltration?

- A. DNS poisoning
- B. URL hijacking
- C. ARP spoofing

D. HTTPS inspection

Answer: A

Explanation:

QUESTION NO: 1436

An administrator must select an algorithm to encrypt data at rest. Which of the following could be used?

- A. RIPEMD
- B. Diffie-hellman
- C. ECDSA
- D. CHAP
- E. Blowfish

Answer: E

Explanation:

QUESTION NO: 1437

RC4 is a strong encryption protocol that is general used with which of the following?

- A. WPA2 CCMP
- B. PEAP
- C. WEP
- D. EAP-TLS

Answer: C

Explanation:

QUESTION NO: 1438

An outside security consultant produces a report of several vulnerabilities for a particular server. Upon further investigation, it is determine that the vulnerability reported does not apply to the platform the server is running on. Which of the following should the consultant do in order to produce more accurate results?

- A. A black box test should be used to increase the validity of the scan
- B. Perform a penetration test in addition to a vulnerability scan
- C. Use banner grabbing to identify the target platform
- D. Use baseline reporting to determine the actual configuration

Answer: B

Explanation:

QUESTION NO: 1439

A programmer has allocated a 32 bit variable to store the results of an operation between two user supplied 4 byte operands. To which of the following types of attack is this application susceptible?

- A. XML injection
- B. Command injection
- C. Integer overflow
- D. Header manipulation

Answer: C

Explanation:

QUESTION NO: 1440

A security administrator is reviewing logs and notices multiple attempts to access the HVAC controls by a workstation with an IP address from the open wireless network. Which of the following would be the best way to prevent this type of attack from occurring again?

- A. Implement VLANs to separate the HVAC
- B. Enable WPA2 security for the wireless network
- C. Install a HIDS to protect the HVAC system
- D. Enable Mac filtering for the wireless network

Answer: D

Explanation:

QUESTION NO: 1441

An application developer needs to allow employees to use their network credentials to access a new application being developed. Which of the following should be configured in the new

application to enable this functionality?

- A. LDAP
- B. ACLs
- C. SNMP
- D. IPSec

Answer: A

Explanation:

QUESTION NO: 1442

During a routine audit it is discovered that someone has been using a state administrator account to log into a seldom used server. The person used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could BEST prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policies
- D. Account expiration policies

Answer: D

Explanation:

QUESTION NO: 1443

A security engineer would like to analyze the effect of deploying a system without patching it to discover potential vulnerabilities. Which of the following practices would best allow for this testing while keeping the corporate network safe?

- A. Perform grey box testing of the system to verify the vulnerabilities on the system
- B. Utilize virtual machine snapshots to restore from compromises
- C. Deploy the system in a sandbox environment on the virtual machine
- D. Create network ACLs that restrict all incoming connections to the system

Answer: C

Explanation:

QUESTION NO: 1444

The internal audit group discovered that unauthorized users are making unapproved changes to various system configuration settings. This issue occurs when previously authorized users transfer from one department to another and maintain the same credentials. Which of the following controls can be implemented to prevent such unauthorized changes in the future?

- A. Periodic access review
- B. Group based privileges
- C. Least privilege
- D. Account lockout

Answer: C

Explanation:

QUESTION NO: 1445

In order to gain an understanding of the latest attack tools being used in the wild, an administrator puts a Unix server on the network with the root users password to set root. Which of the following best describes this technique?

- A. Pharming
- B. Honeypot
- C. Gray box testing
- D. phishing

Answer: B

Explanation:

QUESTION NO: 1446

An administrator, Ann, wants to ensure that only authorized devices are connected to a switch. She decides to control access based on MAC addresses. Which of the following should be configured?

- A. Implicit deny
- B. Private VLANs
- C. Flood guard
- D. Switch port security

Answer: D

Explanation:**QUESTION NO: 1447**

A one time security audit revealed that employees do not have the appropriate access to system resources. The auditor is concerned with the fact that most of the accounts audited have unneeded elevated permission to sensitive resources. Which of the following was implemented to detect this issue?

- A. Continuous monitoring
- B. Account review
- C. Group based privileges
- D. Credential management

Answer: B

Explanation:

QUESTION NO: 1448

A security analyst has a sample of malicious software and needs to know what the sample in a carefully controlled and monitored virtual machine to observe the software's behavior. After the software has run, the analyst returns the virtual machines OS to a pre-defined known good state using what feature of virtualization?

- A. Host elasticity
- B. Antivirus
- C. sandbox
- D. snapshots

Answer: D

Explanation:

QUESTION NO: 1449

Joe, the chief technical officer (CTO) is concerned that the servers and network devices may not be able to handle the growing needs of the company. He has asked his network engineer to begin monitoring the performance of these devices and present statistics to management for capacity planning. Which of the following protocols should be used to this?

- A. SNMP
- B. SSH
- C. TLS
- D. ICMP

Answer: A

Explanation:

QUESTION NO: 1450

A security administrator is responsible for ensuring that there are no unauthorized devices utilizing the corporate network. During a routine scan, the security administrator discovers an unauthorized device belonging to a user in the marketing department. The user is using an android phone in order to browse websites. Which of the following device attributes was used to determine that the device was unauthorized?

- A. An IMEI address
- B. A phone number
- C. A MAC address
- D. An asset ID

Answer: C

Explanation:

QUESTION NO: 1451

A website is breached, exposing the usernames and MD5 password hashes of its entire user base. Many of these passwords are later cracked using rainbow tables. Which of the following actions could have helped prevent the use of rainbow tables on the password hashes?

- A. use salting when computing MD5 hashes of the user passwords
- B. Use SHA as a hashing algorithm instead of MD5
- C. Require SSL for all user logins to secure the password hashes in transit
- D. Prevent users from using a dictionary word in their password

Answer: B

Explanation:

QUESTION NO: 1452

Joe a network administrator is setting up a virtualization host that has additional storage requirements. Which of the following protocols should be used to connect the device to the company SAN? (Select Two)

- A. Fibre channel
- B. SCP
- C. iSCSI
- D. FDDI
- E. SSL

Answer: A,C

Explanation:

QUESTION NO: 1453

A security administrator finds that an intermediate CA within the company was recently breached. The certificates held on this system were lost during the attack, and it is suspected that the attackers had full access to the system. Which of the following is the NEXT action to take in this scenario?

- A. Use a recovery agent to restore the certificates used by the intermediate CA
- B. Revoke the certificate for the intermediate CA
- C. Recover the lost keys from the intermediate CA key escrow
- D. Issue a new certificate for the root CA

Answer: B

Explanation:

QUESTION NO: 1454

A recent online password audit has identified that stale accounts are at risk to brute force attacks. Which the following controls would best mitigate this risk?

- A. Password length
- B. Account disablement
- C. Account lockouts
- D. Password complexity

Answer: C

Explanation:

QUESTION NO: 1455

The security administrator generates a key pair and sends one key inside a rest file to a third party. The third party sends back a signed file. In this scenario, the file sent by the administrator is a:

- A. CA
- B. CRL
- C. KEK
- D. PKI
- E. CSR

Answer: E

Explanation:

QUESTION NO: 1456

Joe, a security technician, is configuring two new firewalls through the web on each. Each time Joe connects, there is a warning message in the browser window about the certificate being untrusted. Which of the following will allow Joe to configure a certificate for the firewall so that firewall administrators are able to connect both firewalls without experiencing the warning message?

- A. Apply a permanent override to the certificate warning in the browser
- B. Apply a wildcard certificate obtained from the company's certificate authority
- C. Apply a self-signed certificate generated by each of the firewalls
- D. Apply a single certificate obtained from a public certificate authority

Answer: C

Explanation:

QUESTION NO: 1457

A company has had their web application become unavailable several times in the past few months due to increased demand. Which of the following should the company perform to increase availability?

- A. Implement a web application firewall to prevent DDoS attacks'
- B. Configure the firewall to work with the IPS to rate limit customer requests
- C. Implement a load balancer to distribute traffic based on back end server utilization
- D. Configure the web server to detect race conditions and automatically restart the web services

Answer: C

Explanation:

QUESTION NO: 1458

A system administrator wants to prevent password compromises from offline password attacks. Which of the following controls should be configured to BEST accomplish this task? (Select TWO)

- A. Password reuse
- B. Password length
- C. Password complexity
- D. Password history
- E. Account lockouts

Answer: C,E

Explanation:

QUESTION NO: 1459

A company recently experienced several security breaches that resulted in confidential data being infiltrated from the network. The forensic investigation revealed that the data breaches were caused by an insider accessing files that resided in shared folders who then encrypted the data and sent it to contacts via third party email. Management is concerned that other employees may also be sending confidential files outside of the company to the same organization. Management has requested that the IT department implement a solution that will allow them to:

Track access and use of files marked confidential, provide documentation that can be used for investigations, prevent employees from sending confidential data via secure third party email, identify other employees that may be involved in these activities.

Which of the following would be the best choice to implement to meet the above requirements?

- A. Web content filtering capable of inspecting and logging SSL traffic used by third party webmail providers
- B. Full disk encryption on all computers with centralized event logging and monitoring enabled
- C. Host based firewalls with real time monitoring and logging enabled

D. Agent-based DLP software with correlations and logging enabled

Answer: D

Explanation:

QUESTION NO: 1460

Which of the following BEST describes malware that tracks a user's web browsing habits and injects the attacker's advertisements into unrelated web pages? (Select TWO)

- A. Logic bomb
- B. Backdoor
- C. Ransomware
- D. Adware
- E. Botnet
- F. Spyware

Answer: C,D

Explanation:

QUESTION NO: 1461

The chief security officer (CSO) has issued a new policy to restrict generic or shared accounts on company systems. Which of the following sections of the policy requirements will have the most impact on generic and shared accounts?

- A. Account lockout
- B. Password length
- C. Concurrent logins
- D. Password expiration

Answer: C

Explanation:

QUESTION NO: 1462

Joe an end user has received a virus detection warning. Which of the following is the first course of action that should be taken?

- A. Recovery
- B. Reporting
- C. Remediation
- D. Identification

Answer: B

Explanation:

QUESTION NO: 1463

A company has several public conference room areas with exposed network outlets. In the past, unauthorized visitors and vendors have used the outlets for internet access. The help desk manager does not want the outlets to be disabled due to the number of training sessions in the conference room and the amount of time it takes to get the ports either patched in or enabled. Which of the following is the best option for meeting this goal?

- A. Flood guards
- B. Port security
- C. 802.1x
- D. Loop protection
- E. IPSec

Answer: C

Explanation:

QUESTION NO: 1464

An attacker unplugs the access point at a coffee shop. The attacker then runs software to make a laptop look like an access point and advertises the same network as the coffee shop normally does. Which of the following describes this type of attack?

- A. IV
- B. Xmas
- C. Packet sniffing
- D. Evil twin
- E. Rouge AP

Answer: D

Explanation:

QUESTION NO: 1465

A network administrator argues that WPA2 encryption is not needed, as MAC filtering is enabled on the access point. Which of the following would show the administrator that wpa2 is also needed?

- A. Deploy an evil twin with mac filtering
- B. Flood access point with random mac addresses
- C. Sniff and clone a mac address
- D. DNS poison the access point

Answer: C

Explanation:

QUESTION NO: 1466

A security director has contracted an outside testing company to evaluate the security of a newly developed application. None of the parameters or internal workings of the application have been provided to the testing company prior to the start of testing. The testing company will be using:

- A. Gray box testing
- B. Active control testing
- C. White box testing
- D. Black box testing

Answer: D

Explanation:

QUESTION NO: 1467

While preparing for an audit a security analyst is reviewing the various controls in place to secure the operation of financial processes within the organization. Based on the pre assessment report, the department does not effectively maintain a strong financial transaction control environment due to conflicting responsibilities held by key personnel. If implemented, which of the following security concepts will most effectively address the finding?

- A. Least privilege
- B. Separation of duties
- C. Time-based access control
- D. Dual control

Answer: B

Explanation:

QUESTION NO: 1468

A chief privacy officer, Joe, is concerned that employees are sending emails to addresses outside of the company that contain PII. He asks that the security technician to implement technology that will mitigate this risk. Which of the following would be the best option?

- A. DLP
- B. HIDS
- C. Firewall
- D. Web content filtering

Answer: A

Explanation:

QUESTION NO: 1469

The key management organization has implemented a key escrowing function. Which of the following technologies can provide protection for the PKI's escrowed keys?

- A. CRL
- B. OCSP
- C. TPM
- D. HSM

Answer: A

Explanation:

QUESTION NO: 1470

Which of the following are unique to white box testing methodologies? (Select two)

- A. Application program interface API testing
- B. Bluesnarfing
- C. External network penetration testing
- D. Function, statement and code coverage

E. Input fuzzing

Answer: A,D

Explanation:

QUESTION NO: 1471

A technician installed two ground plane antennae on 802.11n bridges connecting two buildings 500 feet apart. After configuring both radios to work at 2.4ghz and implementing the correct configuration, connectivity tests between the two buildings are unsuccessful. Which of the following should the technician do to resolve the connectivity problem?

- A. Substitute wireless bridges for wireless access points
- B. Replace the 802.11n bridges with 802.11ac bridges
- C. Configure both bridges to use 5GHz instead of 2.4GHz
- D. Replace the current antennae with Yagi antennae

Answer: D

Explanation:

QUESTION NO: 1472

A company has had several security incidents in the past six months. It appears that the majority of the incidents occurred on systems with older software on development workstations. Which of the following should be implemented to help prevent similar incidents in the future?

- A. Peer code review
- B. Application whitelisting
- C. Patch management
- D. Host-based firewall

Answer: C

Explanation:

QUESTION NO: 1473

A router was shut down as a result of a DoS attack. Upon review of the router logs, it was determined that the attacker was able to connect to the router using a console cable to complete the attack. Which of the following should have been implemented on the router to prevent this

attack? (Select two)

- A. IP ACLs should have been enabled on the console port on the router
- B. Console access to the router should have been disabled
- C. Passwords should have been enabled on the virtual terminal interfaces on the router
- D. Virtual terminal access to the router should have been disabled
- E. Physical access to the router should have been restricted

Answer: B,E

Explanation:

QUESTION NO: 1474

A systems administrator is configuring a new file server and has been instructed to configure writeable to by the department manager, and read only for the individual employee. Which of the following is the name for the access control methodology used?

- A. Duty separation
- B. Mandatory
- C. Least privilege
- D. Role-based

Answer: D

Explanation:

QUESTION NO: 1475

An administrator is implementing a security control that only permits the execution of allowed programs. Which of the following are cryptography concepts that should be used to identify the allowed programs? (Select two.)

- A. Digital signatures
- B. Hashing
- C. Asymmetric encryption
- D. openID
- E. key escrow

Answer: A,B

Explanation:

QUESTION NO: 1476

While responding to an incident on a Linux server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

- A. Lsof
- B. Tcpdump
- C. Top
- D. Ifconfig

Answer: A

Explanation:

QUESTION NO: 1477

A bank chief information security officer (CISO) is responsible for a mobile banking platform that operates natively on iOS and Android. Which of the following security controls helps protect the associated publicly accessible API endpoints?

- A. Mobile device management
- B. Jailbreak detection
- C. Network segmentation
- D. Application firewalls

Answer: D

Explanation:

QUESTION NO: 1478

A company is rolling out a new e-commerce website. The security analyst wants to reduce the risk of the new website being comprised by confirming that system patches are up to date, application hot fixes are current, and unneeded ports and services have been disabled. To do this, the security analyst will perform a:

- A. Vulnerability assessment
- B. White box test
- C. Penetration test

D. Peer review

Answer: A

Explanation:

QUESTION NO: 1479

Joe, a security analyst, is attempting to determine if a new server meets the security requirements of his organization. As a step in this process, he attempts to identify a lack of security controls and to identify common misconfigurations on the server. Which of the following is Joe attempting to complete?

- A. Black hat testing
- B. Vulnerability scanning
- C. Black box testing
- D. Penetration testing

Answer: B

Explanation:

QUESTION NO: 1480

A classroom utilizes workstations running virtualization software for a maximum of one virtual machine per working station. The network settings on the virtual machines are set to bridged. Which of the following describes how the switch in the classroom should be configured to allow for the virtual machines and host workstation to connect to network resources?

- A. The maximum-mac settings of the ports should be set to zero
- B. The maximum-mac settings of the ports should be set to one
- C. The maximum-mac settings of the ports should be set to two
- D. The maximum mac settings of the ports should be set to three

Answer: A

Explanation:

QUESTION NO: 1481

Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?

- A. Replay
- B. Smurf
- C. Xmas
- D. Fraggle

Answer: C

Explanation:

QUESTION NO: 1482

A Company transfers millions of files a day between their servers. A programmer for the company has created a program that indexes and verifies the integrity of each file as it is replicated between servers. The programmer would like to use the fastest algorithm to ensure integrity. Which of the following should the programmer use?

- A. SHA1
- B. RIPEMD
- C. DSA
- D. MD5

Answer: D

Explanation:

QUESTION NO: 1483

A system administrator is conducting baseline audit and determines that a web server is missing several critical updates. Which of the following actions should the administrator perform first to correct the issue?

- A. Open a service ticket according to the patch management plan
- B. Disconnect the network interface and use the administrative management console to perform the updates
- C. Perform a backup of the server and install the require patches
- D. Disable the services for the web server but leave the server alone pending patch updates

Answer: A

Explanation:

QUESTION NO: 1484

The IT department has been tasked with reducing the risk of sensitive information being shared with unauthorized entities from computers it is saved on, without impeding the ability of the employees to access the internet. Implementing which of the following would be the best way to accomplish this objective?

- A. Host-based firewalls
- B. DLP
- C. URL filtering
- D. Pop-up blockers

Answer: B

Explanation:

QUESTION NO: 1485

A server crashes at 6 pm. Senior management has determined that data must be restored within two hours of a server crash. Additionally, a loss of more than one hour worth of data is detrimental to the company's financial well-being. Which of the following is the RTO?

- A. 7pm
- B. 8pm
- C. 9pm
- D. 10pm

Answer: B

Explanation:

QUESTION NO: 1486

To mitigate the risk of intrusion, an IT Manager is concerned with using secure versions of protocols and services whenever possible. In addition, the security technician is required to monitor the types of traffic being generated. Which of the following tools is the technician MOST likely to use?

- A. Port scanner
- B. Network analyzer
- C. IPS
- D. Audit Logs

Answer: B

Explanation:

QUESTION NO: 1487

An administrator is implementing a new management system for the machinery on the company's production line. One requirement is that the system only be accessible while within the production facility. Which of the following will be the MOST effective solution in limiting access based on this requirement?

- A. Access control list
- B. Firewall policy
- C. Air Gap
- D. MAC filter

Answer: A

Explanation:

QUESTION NO: 1488

A risk assessment team is concerned about hosting data with a cloud service provider (CSP) which of the following findings would justify this concern?

- A. The CPS utilizes encryption for data at rest and in motion
- B. The CSP takes into account multinational privacy concerns
- C. The financial review indicates the company is a startup
- D. SLA state service tickets will be resolved in less than 15 minutes

Answer: B

Explanation:

QUESTION NO: 1489

A company wishes to prevent unauthorized employee access to the data center. Which of the following is the MOST secure way to meet this goal?

- A. Use Motion detectors to signal security whenever anyone entered the center
- B. Mount CCTV cameras inside the center to monitor people as they enter

- C. Install mantraps at every entrance to the data center in conjunction with their badges
- D. Place biometric readers at the entrances to verify employees' identity

Answer: C

Explanation:

QUESTION NO: 1490

A company hosts a web server that requires entropy in encryption initialization and authentication. To meet this goal, the company would like to select a block cipher mode of operation that allows an arbitrary length IV and supports authenticated encryption. Which of the following would meet these objectives?

- A. CFB
- B. GCM
- C. ECB
- D. CBC

Answer: C

Explanation:

QUESTION NO: 1491

A chief information security officer (CISO) is providing a presentation to a group of network engineers. In the presentation, the CISO presents information regarding exploit kits. Which of the following might the CISO present?

- A. Exploit kits are tools capable of taking advantage of multiple CVEs
- B. Exploit kits are vulnerability scanners used by penetration testers
- C. Exploit kits are WIFI scanning tools that can find new honeypots
- D. Exploit kits are a new type of malware that allow attackers to control their computers

Answer: A

Explanation:

QUESTION NO: 1492

During a company-wide initiative to harden network security, it is discovered that end users who have laptops cannot be removed from the local administrator group. Which of the following could

be used to help mitigate the risk of these machines becoming compromised?

- A. Security log auditing
- B. Firewalls
- C. HIPS
- D. IDS

Answer: B

Explanation:

QUESTION NO: 1493

An administrator receives a security alert that appears to be from one of the company's vendors. The email contains information and instructions for patching a serious flaw that has not been publicly announced. Which of the following can an employee use to validate the authenticity of the email?

- A. Hashing algorithm
- B. Ephemeral Key
- C. SSL certificate chain
- D. Private key
- E. Digital signature

Answer: A

Explanation:

QUESTION NO: 1494

A project team is developing requirements of the new version of a web application used by internal and external users. The application already features username and password requirements for login, but the organization is required to implement multifactor authentication to meet regulatory requirements. Which of the following would be added requirements will satisfy the regulatory requirement? (Select THREE.)

- A. Digital certificate
- B. Personalized URL
- C. Identity verification questions
- D. Keystroke dynamics
- E. Tokenized mobile device
- F. Time-of-day restrictions

- G. Increased password complexity
- H. Rule-based access control

Answer: A,C,E

Explanation:

QUESTION NO: 1495

A bank is planning to implement a third factor to protect customer ATM transactions. Which of the following could the bank implement?

- A. SMS
- B. Fingerprint
- C. Chip and Pin
- D. OTP

Answer: C

Explanation:

QUESTION NO: 1496

Which of the following internal security controls is aimed at preventing two system administrators from completing the same tasks?

- A. Least privilege
- B. Separation of Duties
- C. Mandatory Vacation
- D. Security Policy

Answer: B

Explanation:

QUESTION NO: 1497

An administrator performs a risk calculation to determine if additional availability controls need to be in place. The administrator estimates that a server fails and needs to be replaced once every 2 years at a cost of \$8,000. Which of the following represents the factors that the administrator would use to facilitate this calculation?

- A. ARO= 0.5; SLE= \$4,000; ALE= \$2,000
- B. ARO=0.5; SLE=\$8,000; ALE=\$4,000
- C. ARO=0.5; SLE= \$4,000; ALE=\$8,000
- D. ARO=2; SLE= \$4,000; ALE=\$8,000
- E. ARO=2; SLE= \$8,000; ALE= \$16,000

Answer: B

Explanation:

QUESTION NO: 1498

A security administrator needs to implement a technology that creates a secure key exchange. Neither party involved in the key exchange will have pre-existing knowledge of one another. Which of the following technologies would allow for this?

- A. Blowfish
- B. NTLM
- C. Diffie-Hellman
- D. CHAP

Answer: C

Explanation:

QUESTION NO: 1499

A technician has been assigned a service request to investigate a potential vulnerability in the organization's extranet platform. Once the technician performs initial investigative measures, it is determined that the potential vulnerability was a false-alarm. Which of the following actions should the technician take in regards to the findings?

- A. Write up the findings and disable the vulnerability rule in future vulnerability scans
- B. Refer the issue to the server administrator for resolution
- C. Mark the finding as a false-negative and close the service request
- D. Document the results and report the findings according to the incident response plan

Answer: D

Explanation:

QUESTION NO: 1500

A security administrator is using a software program to test the security of a wireless access point. After running the program for a few hours, the access point sends the wireless secret key back to the software program. Which of the following attacks is this an example of?

- A. WPS
- B. IV
- C. Deauth
- D. Replay

Answer: C

Explanation:

QUESTION NO: 1501

A user, Ann, has been issued a smart card and is having problems opening old encrypted email. Ann published her certificates to the local windows store and to the global address list. Which of the following would still need to be performed?

- A. Setup the email security with her new certificates
- B. Recover her old private certificate
- C. Reinstall her previous public certificate
- D. Verify the correct email address is associated with her certificate

Answer: A

Explanation:

QUESTION NO: 1502

Which of the following is a best practice when setting up a client to use the LDAPS protocol with a server?

- A. The client should follow LDAP referrals to other secure servers on the network
- B. The client should trust the CA that signed the server's certificate
- C. The client should present a self-signed certificate to the server
- D. The client should have access to port 389 on the server

Answer: C

Explanation:

QUESTION NO: 1503

A network manager needs a cost-effective solution to allow for the restoration of information with a RPO of 24 hours. The disaster recovery plan also requires that backups occur within a restricted timeframe during the week and be take offsite weekly. Which of the following should the manager choose to BEST address these requirements?

- A. Daily incremental backup to tape
- B. Disk-to-disk hourly server snapshots
- C. Replication of the environment at a hot site
- D. Daily differential backup to tape
- E. Daily full backup to tape

Answer: A

Explanation:

QUESTION NO: 1504

Given the following set of firewall rules:

From the inside to outside allow source any destination any port any

From inside to dmz allow source any destination any port tcp-80

From inside to dmz allow source any destination any port tcp-443

Which of the following would prevent FTP traffic from reaching a server in the DMZ from the inside network?

- A. Implicit deny
- B. Policy routing
- C. Port forwarding
- D. Forwarding proxy

Answer: A

Explanation:

QUESTION NO: 1505

During a routine configuration audit, a systems administrator determines that a former employee placed an executable on an application server. Once the system was isolated and diagnosed, it was determined that the executable was programmed to establish a connection to a malicious command and control server. Which of the following forms of malware is best described in the scenario?

- A. Logic bomb
- B. Rootkit
- C. Back door
- D. Ransomware

Answer: B

Explanation:

QUESTION NO: 1506

The chief information officer (CIO) of a major company intends to increase employee connectivity and productivity by issuing employees mobile devices with access to their enterprise email, calendar, and contacts. The solution the CIO intends to use requires a PKI that automates the enrollment of mobile device certificates. Which of the following, when implemented and configured securely, will meet the CIO's requirement?

- A. OCSP
- B. SCEP
- C. SAML
- D. OSI

Answer: B

Explanation:

QUESTION NO: 1507

An attacker impersonates a fire marshal and demands access to the datacenter under the threat of a fine. Which of the following reasons make this effective? (Select two.)

- A. Consensus
- B. Authority
- C. Intimidation
- D. Trust

E. Scarcity

Answer: B,E

Explanation:

QUESTION NO: 1508

In the course of troubleshooting wireless issues from users a technician discovers that users are connecting to their home SSIDs which the technician scans but detects none of these SSIDs. The technician eventually discovers a rouge access point that spoofs any SSID request. Which of the following allows wireless use while mitigating this type of attack?

- A. Configure the device to verify access point MAC addresses
- B. Disable automatic connection to known SSIDs
- C. Only connect to trusted wireless networks
- D. Enable MAC filtering on the wireless access point

Answer: A

Explanation:

QUESTION NO: 1509

Which of the following describes the implementation of PAT?

- A. Translating the source and destination IPS, but not the source and destination ports
- B. A one to one persistent mapping between on private IP and one Public IP
- C. Changing the priority of a TCP stream based on the source address
- D. Associating multiple public IP addresses with one private address

Answer: D

Explanation:

QUESTION NO: 1510

Which of the following forms of software testing can best be performed with no knowledge of how a system is internally structured or functions? (Select Two.)

- A. Boundary testing

- B. White box
- C. Fuzzing
- D. Black box
- E. Grey Box

Answer: C,D

Explanation:

QUESTION NO: 1511

A load balancer has the ability to remember which server a particular client is using and always directs that client to the same server. This feature is called:

- A. Cookie tracking
- B. URL filtering
- C. Session affinity
- D. Behavior monitoring

Answer: C

Explanation:

QUESTION NO: 1512

A company has recently begun to provide internal security awareness for employees. Which of the following would be used to demonstrate the effectiveness of the training?

- A. Metrics
- B. Business impact analysis
- C. Certificate of completion
- D. Policies

Answer: C

Explanation:

QUESTION NO: 1513

Users in an organization are experiencing when attempting to access certain websites. The users report that when they type in a legitimate URL, different boxes appear on the screen, making it difficult to access the legitimate sites. Which of the following would best mitigate this issue?

- A. Pop-up blockers
- B. URL filtering
- C. Antivirus
- D. Anti-spam

Answer: C

Explanation:

QUESTION NO: 1514

A company hires a penetration testing team to test its overall security posture. The organization has not disclosed any information to the penetration testing team and has allocated five days for testing. Which of the following types of testing will the penetration testing team have to conduct?

- A. Static analysis
- B. Gray Box
- C. White box
- D. Black box

Answer: D

Explanation:

QUESTION NO: 1515

A web administrator has just implemented a new web server to be placed in production. As part of the company's security plan, any new system must go through a security test before it is placed in production. The security team runs a port scan resulting in the following data:

- 21 tcp open FTP
- 23 tcp open Telnet
- 22 tcp open SSH
- 25 UDP open smtp
- 110 tcp open pop3
- 443 tcp open https

Which of the following is the BEST recommendation for the web administrator?

- A. Implement an IPS
- B. Disable unnecessary services
- C. Disable unused accounts
- D. Implement an IDS
- E. Wrap TELNET in SSL

Answer: B

Explanation:

QUESTION NO: 1516

Which of the following best describes the reason for using hot and cold aisles?

- A. To ensure air exhaust from one aisle doesn't blow into the air intake of the next aisle
- B. To ensure the dewpoint stays low enough that water doesn't condensate on equipment
- C. To decrease amount of power wiring that is run to each aisle
- D. Too maintain proper humidity in the datacenter across all aisles

Answer: A

Explanation:

QUESTION NO: 1517

An organization has an internal PKI that utilizes client certificates on each workstation. When deploying a new wireless network, the security engineer has asked that the new network authenticate clients by utilizes the existing client certificates. Which of the following authentication mechanisms should be utilized to meet this goal?

- A. EAP-FAST
- B. LEAP
- C. PEAP
- D. EAP-TLS

Answer: B

Explanation:

QUESTION NO: 1518

An attacker is attempting to insert malicious code into an installer file that is available on the

internet. The attacker is able to gain control of the web server that houses both the installer and the web page which features information about the downloadable file. To implement the attack and delay detection, the attacker should modify both the installer file and the:

- A. SSL certificate on the web server
- B. The HMAC of the downloadable file available on the website
- C. Digital signature on the downloadable file
- D. MD5 hash of the file listed on the website

Answer: D

Explanation:

QUESTION NO: 1519

After receiving the hard drive from detectives, the forensic analyst for a court case used a log to capture corresponding events prior to sending the evidence to lawyers. Which of the following do these actions demonstrate?

- A. Chain of custody
- B. Order of volatility
- C. Data analysis
- D. Tracking man hours and expenses

Answer: A

Explanation:

QUESTION NO: 1520

A group of users from multiple departments are working together on a project and will maintain their digital output in a single location. Which of the following is the BEST method to ensure access is restricted to use by only these users?

- A. Mandatory access control
- B. Rule-based access
- C. Group based privileges
- D. User assigned privileges

Answer: D

Explanation:

QUESTION NO: 1521

Which of the following technologies when applied to android and iOS environments, can an organization use to add security restrictions and encryption to existing mobile applications? (Select Two)

- A. Mobile device management
- B. Containerization
- C. Application whitelisting
- D. Application wrapping
- E. Mobile application store

Answer: A,C

Explanation:

QUESTION NO: 1522

A server administrator discovers the web farm is using weak ciphers and wants to ensure that only stronger ciphers are accepted. Which of the following ciphers should the administrator implement in the load balancer? (Select Two)

- A. SHA-129
- B. DES
- C. MD5
- D. RC4
- E. CRC-32

Answer: A,D

Explanation:

QUESTION NO: 1523

An application developer has coded a new application with a module to examine all user entries for the graphical user interface. The module verifies that user entries match the allowed types for each field and that OS and database commands are rejected before entries are sent for further processing within the application. These are example of:

- A. Input validation

- B. SQL injection
- C. Application whitelisting
- D. Error handling

Answer: A

Explanation:

QUESTION NO: 1524

Ann, a security administrator is hardening the user password policies. She currently has the following in place.

Passwords expire every 60 days

Password length is at least eight characters

Passwords must contain at least one capital letter and one numeric character

Passwords cannot be reused until the password has been changed eight times

She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?

- A. Lower the password expiry time to every 30days instead of every 60 days
- B. Require that the password contains at least one capital, one numeric, and one special character
- C. Change the re-usage time from eight to 16 changes before a password can be repeated
- D. Create a rule that users can only change their passwords once every two weeks

Answer: D

Explanation:

QUESTION NO: 1525

Which of the following BEST describes disk striping with parity?

- A. RAID 0
- B. RAID 1
- C. RAID 2
- D. RAID 5

Answer: D

Explanation:

QUESTION NO: 1526

Which of the following will allow the live state of the virtual machine to be easily reverted after a failed upgrade?

- A. Replication
- B. Backups
- C. Fault tolerance
- D. Snapshots

Answer: D

Explanation:

QUESTION NO: 1527

An organization currently uses FTP for the transfer of large files, due to recent security enhancements, is now required to use a secure method of file transfer and is testing both SFTP and FTPS as alternatives. Which of the following ports should be opened on the firewall in order to test the two alternatives? (Select Two)

- A. TCP 22
- B. TCP 25
- C. TCP 69
- D. UDP 161
- E. TCP 990
- F. TCP 3380

Answer: A,E

Explanation:

QUESTION NO: 1528

Which of the following types of malware, attempts to circumvent malware detection by trying to hide its true location on the infected system?

- A. Armored virus
- B. Ransomware
- C. Trojan
- D. Keylogger

Answer: C

Explanation:

QUESTION NO: 1529

An attacker went to a local bank and collected disposed paper for the purpose of collecting data that could be used to steal funds and information from the bank's customers. This is an example of:

- A. Impersonation
- B. Whaling
- C. Dumpster diving
- D. Hoaxes

Answer: C

Explanation:

QUESTION NO: 1530

An employee reports work was being completed on a company owned laptop using a public wireless hot-spot. A pop-up screen appeared and the user closed the pop-up. Seconds later the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

- A. Ransomware
- B. Rootkit
- C. Scareware
- D. Spyware

Answer: A

Explanation:

QUESTION NO: 1531

A small IT security firm has an internal network composed of laptops, servers, and printers. The network has both wired and wireless segments and supports VPN access from remote sites. To protect the network from internal and external threats, including social engineering attacks, the company decides to implement stringent security controls. Which of the following lists is the BEST combination of security controls to implement?

- A.** Disable SSID broadcast, require full disk encryption on servers, laptop, and personally owned electronic devices, enable MAC filtering on WAPs, require photographic ID to enter the building.
- B.** Enable port security; divide the network into segments for servers, laptops, public and remote users; apply ACLs to all network equipment; enable MAC filtering on WAPs; and require two-factor authentication for network access.
- C.** Divide the network into segments for servers, laptops, public and remote users; require the use of one time pads for network key exchange and access; enable MAC filtering ACLs on all servers.
- D.** Enable SSID broadcast on a honeynet; install monitoring software on all corporate equipment; install CCTVs to deter social engineering; enable SELinux in permissive mode.

Answer: B

Explanation:

QUESTION NO: 1532

A security analyst is working on a project team responsible for the integration of an enterprise SSO solution. The SSO solution requires the use of an open standard for the exchange of authentication and authorization across numerous web based applications. Which of the following solutions is most appropriate for the analyst to recommend in this scenario?

- A.** SAML
- B.** XTACACS
- C.** RADIUS
- D.** TACACS+
- E.** Secure LDAP

Answer: A

Explanation:

QUESTION NO: 1533

A thief has stolen a mobile device and removed its battery to circumvent GPS location tracking. The device user is a four digit PIN. Which of the following is a mobile device security control that

ensures the confidentiality of company data?

- A. Remote wiping
- B. Mobile Access control
- C. Full device encryption
- D. Inventory control

Answer: C

Explanation:

QUESTION NO: 1534

A user has called the help desk to report an enterprise mobile device was stolen. The technician receiving the call accesses the MDM administration portal to identify the device's last known geographic location. The technician determines the device is still communicating with the MDM. After taking note of the last known location, the administrator continues to follow the rest of the checklist. Which of the following identifies a possible next step for the administrator?

- A. Remotely encrypt the device
- B. Identify the mobile carrier's IP address
- C. Reset the device password
- D. Issue a remote wipe command

Answer: D

Explanation:

QUESTION NO: 1535

A risk management team indicated an elevated level of risk due to the location of a corporate datacenter in a region with an unstable political climate. The chief information officer (CIO) accepts the recommendation to transition the workload to an alternate datacenter in a more stable region. Which of the following forms of risk mitigation has the CIO elected to pursue?

- A. Deterrence
- B. Transference
- C. Avoidance
- D. Acceptance
- E. sharing

Answer: C

Explanation:**QUESTION NO: 1536**

During a recent audit, the auditors cited the company's current virtual machine infrastructure as a concern. The auditors cited the fact that servers containing sensitive customer information reside on the same physical host as numerous virtual machines that follow less stringent security guidelines. Which of the following would be the best choice to implement to address this audit concern while maintain the current infrastructure?

- A.** Migrate the individual virtual machines that do not contain sensitive data to separate physical machines
- B.** Implement full disk encryption on all servers that do not contain sensitive customer data
- C.** Move the virtual machines that contain the sensitive information to a separate host
- D.** Create new VLANs and segment the network according to the level of data sensitivity

Answer: D

Explanation:**QUESTION NO: 1537**

A switch is set up to allow only 2 simultaneous MAC addresses per switch port. An administrator is reviewing a log and determines that a switch port has been deactivated in a conference room after it detected 3 or more MAC addresses on the same port. Which of the following reasons could have caused this port to be disabled?

- A.** A pc had a NIC replaced and reconnected to the switch
- B.** An ip telephone has been plugged in
- C.** A rogue access point was plugged in
- D.** An arp attack was launched from a pc on this port

Answer: D

Explanation:**QUESTION NO: 1538**

A network administrator was to implement a solution that will allow authorized traffic, deny unauthorized traffic and ensure that appropriate ports are being used for a number of TCP and

UDP protocols. Which of the following network controls would meet these requirements?

- A. Stateful firewall
- B. Web security gateway
- C. URL filter
- D. proxy server
- E. web application firewall

Answer: A

Explanation:

QUESTION NO: 1539

Client computers login at specified times to check and update antivirus definitions using a dedicated account configured by the administrator. One day the clients are unable to login with the account, but the server still responds to ping requests. The administrator has not made any changes. Which of the following most likely happened?

- A. Group policy is blocking the connection attempts
- B. The administrator account has been disabled
- C. The switch port for the server has died
- D. The password on the account has expired

Answer: D

Explanation:

QUESTION NO: 1540

In performing an authorized penetration test of an organization's system security, a penetration tester collects information pertaining to the application versions that reside on a server. Which of the following is the best way to collect this type of information?

- A. Protocol analyzer
- B. Banner grabbing
- C. Port scanning
- D. Code review

Answer: B

Explanation:

QUESTION NO: 1541

a company is deploying an new video conferencing system to be used by the executive team for board meetings. The security engineer has been asked to choose the strongest available asymmetric cipher to be used for encryption of board papers, and chose the strongest available stream cipher to be configured for video streaming. Which of the following ciphers should be chosen? (Select two)

- A. RSA
- B. RC4
- C. 3DES
- D. HMAC
- E. SJA-256

Answer: A,B

Explanation:

QUESTION NO: 1542

Joe has hired several new security administrators and have been explaining the design of the company's network. He has described the position and descriptions of the company's firewalls, IDS sensors, antivirus server, DMZs, and HIPS. Which of the following best describes the incorporation of these elements?

- A. Load balancers
- B. Defense in depth
- C. Network segmentation
- D. UTM security appliance

Answer: B

Explanation:

QUESTION NO: 1543

A security administrator is selecting an MDM solution for an organization, which has strict security requirements for the confidentiality of its data on end user devices. The organization decides to allow BYOD, but requires that users wishing to participate agree to the following specific device configurations; camera disablement, password enforcement, and application whitelisting. The organization must be able to support a device portfolio of differing mobile operating systems.

Which of the following represents the MOST relevant technical security criteria for the MDM?

- A. Breadth of support for device manufacturers' security configuration APIs
- B. Ability to extend the enterprise password policies to the chosen MDM
- C. Features to support the backup and recovery of the stored corporate data
- D. Capability to require the users to accept an AUP prior to device onboarding

Answer: B

Explanation:

QUESTION NO: 1544

Employees are reporting that they have been receiving a large number of emails advertising products and services. Links in the email direct the users' browsers to the websites for the items being offered. No reports of increased virus activity have been observed. A security administrator suspects that the users are the targets of:

- A. A watering hole attack
- B. Spear phishing
- C. A spoofing attack
- D. A spam campaign

Answer: D

Explanation:

QUESTION NO: 1545

An employee finds a usb drive in the employee lunch room and plugs the drive into a shared workstation to determine who owns the drive. When the drive is inserted, a command prompt opens and a script begins to run. The employee notifies a technician who determines that data on a server have been compromised. This is an example of:

- A. Device removal
- B. Data disclosure
- C. Incident identification
- D. Mitigation steps

Answer: C

Explanation:

QUESTION NO: 1546

A chief information officer (CIO) is concerned about PII contained in the organization's various data warehouse platforms. Since not all of the PII transferred to the organization is required for proper operation of the data warehouse application, the CIO requests the in needed PII data be parsed and securely discarded. Which of the following controls would be MOST appropriate in this scenario?

- A. Execution of PII data identification assessments
- B. Implementation of data sanitization routines
- C. Encryption of data-at-rest
- D. Introduction of education programs and awareness training
- E. Creation of policies and procedures

Answer: E

Explanation:

QUESTION NO: 1547

The security administrator receives a service ticket saying a host based firewall is interfering with the operation of a new application that is being tested in development. The administrator asks for clarification on which ports need to be open. The software vendor replies that it could use up to 20 ports and many customers have disabled the host based firewall. After examining the system the administrator sees several ports that are open for database and application servers that only used locally. The vendor continues to recommend disabling the host based firewall. Which of the following is the best course of action for the administrator to take?

- A. Allow ports used by the application through the network firewall
- B. Allow ports used externally through the host firewall
- C. Follow the vendor recommendations and disable the host firewall
- D. Allow ports used locally through the host firewall

Answer: D

Explanation:

QUESTION NO: 1548

A corporate wireless guest network uses an open SSID with a captive portal to authenticate guest users. Guests can obtain their portal password at the service desk. A security consultant alerts the

administrator that the captive portal is easily bypassed, as long as one other wireless guest user is on the network. Which of the following attacks did the security consultant use?

- A. ARP poisoning
- B. DNS cache poisoning
- C. MAC spoofing
- D. Rouge DHCP server

Answer: C

Explanation:

QUESTION NO: 1549

A company requires that all wireless communication be compliant with the Advanced encryption standard. The current wireless infrastructure implements WEP + TKIP. Which of the following wireless protocols should be implemented?

- A. CCMP
- B. 802.1x
- C. 802.3
- D. WPA2
- E. AES

Answer: B

Explanation:

QUESTION NO: 1550

A security analyst, while doing a security scan using packet capture security tools, noticed large volumes of data images of company products being exfiltrated to foreign IP addresses. Which of the following is the FIRST step in responding to scan results?

- A. Incident identification
- B. Implement mitigation
- C. Chain of custody
- D. Capture system image

Answer: B

Explanation:

QUESTION NO: 1551

An administrator deploys a WPA2 Enterprise wireless network with EAP-PEAP-MSCHAPv2. The deployment is successful and company laptops are able to connect automatically with no user intervention. A year later, the company begins to deploy phones with wireless capabilities. Users report that they are receiving a warning when they attempt to connect to the wireless network from their phones. Which of the following is the MOST likely cause of the warning message?

- A. Mutual authentication on the phone is not compatible with the wireless network
- B. The phones do not support WPA2 Enterprise wireless networks
- C. User certificates were not deployed to the phones
- D. The phones' built in web browser is not compatible with the wireless network
- E. Self-signed certificates were used on the RADIUS servers

Answer: B

Explanation:

QUESTION NO: 1552

An attacker has gained access to the company's web server by using the administrator's credentials. The attacker then begins to work on compromising the sensitive data on other servers. Which of the following BEST describes this type of attack?

- A. Privilege escalation
- B. Client-side attack
- C. Man-in-the-middle
- D. Transitive access

Answer: B

Explanation:

QUESTION NO: 1553

A security technician is concerned there is not enough security staff available the web servers and database server located in the DMZ around the clock. Which of the following technologies, when deployed, would provide the BEST round the clock automated protection?

- A. HIPS & SIEM

- B. NIPS & HIDS
- C. HIDS& SIEM
- D. NIPS&HIPS

Answer: B

Explanation:

QUESTION NO: 1554

Which of the following best describes the objectives of succession planning?

- A. To identify and document the successive order in which critical systems should be reinstated following a disaster situation
- B. To ensure that a personnel management plan is in place to ensure continued operation of critical processes during an incident
- C. To determine the appropriate order in which contract internal resources, third party suppliers and external customers during a disaster response
- D. To document the order that systems should be reinstated at the primary site following a failover operation at a backup site.

Answer: A

Explanation:

QUESTION NO: 1555

A system administrator wants to use open source software but is worried about the source code being comprised. As a part of the download and installation process, the administrator should verify the integrity of the software by:

- A. Creating a digital signature of the file before installation
- B. Using a secure protocol like HTTPS to download the file
- C. Checking the has against an official mirror that contains the same file
- D. Encryption any connections the software makes

Answer: C

Explanation:

QUESTION NO: 1556

The chief security officer (CSO) has reported a rise in data loss but no break-ins have occurred. By doing which of the following would the CSO MOST likely to reduce the number of incidents?

- A. Implement protected distribution
- B. Employ additional firewalls
- C. Conduct security awareness training
- D. Install perimeter barricades

Answer: C

Explanation:

QUESTION NO: 1557

In an effort to test the effectiveness of an organization's security awareness training, a penetrator tester crafted an email and sent it to all of the employees to see how many of them clicked on the enclosed links. Which of the following is being tested?

- A. How many employees are susceptible to a SPAM attack
- B. How many employees are susceptible to a cross-site scripting attack
- C. How many employees are susceptible to a phishing attack
- D. How many employees are susceptible to a vishing attack

Answer: A

Explanation:

QUESTION NO: 1558

Devices on the SCADA network communicate exclusively at Layer 2. Which of the following should be used to prevent unauthorized systems using ARP-based attacks to compromise the SCADA network?

- A. Application firewall
- B. IPSec
- C. Hardware encryption
- D. VLANs

Answer: B

Explanation:

QUESTION NO: 1559

When information is shared between two separate organizations, which of the following documents would describe the sensitivity as well as the type and flow of the information?

- A. SLA
- B. ISA
- C. BPA
- D. MOA

Answer: D

Explanation:

QUESTION NO: 1560

Joe noticed that there is a larger than normal account of network on the printer VLAN of his organization, causing users to have to wait a long time for a print job. Upon investigation Joe discovers that printers were ordered and added to the network without his knowledge. Which of the following will reduce the risk of this occurring again in the future?

- A. Log analysis
- B. Loop protection
- C. Access control list
- D. Rule-based management

Answer: D

Explanation:

QUESTION NO: 1561

Jo an employee reports to the security manager that several files in a research and development folder that only JOE has access to have been improperly modified. The modified data on the files in recent and the modified by account is Joe's. The permissions on the folder have not been changed, and there is no evidence of malware on the server hosting the folder or on Joe's workstation. Several failed login attempts to Joe's account were discovered in the security log of the LDAP server. Given this scenario, which of the following should the security manager implement to prevent this in the future?

- A. Generic account prohibition
- B. Account lockout
- C. Password complexity

D. User access reviews

Answer: B

Explanation:

QUESTION NO: 1562

A user contacts the help desk after being unable to log in to a corporate website. The user can log into the site from another computer in the next office, but not from the PC. The user's PC was able to connect earlier in the day. The help desk has user restart the NTP service. Afterwards the user is able to log into the website. The MOST likely reason for the initial failure was that the website was configured to use which of the following authentication mechanisms?

- A. Secure LDAP
- B. RADIUS
- C. NTLMv2
- D. Kerberos

Answer: D

Explanation:

QUESTION NO: 1563

A security analyst has been investigating an incident involving the corporate website. Upon investigation, it has been determined that users visiting the corporate website would be automatically redirected to a, malicious site. Further investigation on the corporate website has revealed that the home page on the corporate website has been altered to include an unauthorized item. Which of the following would explain why users are being redirected to the malicious site?

- A. DNS poisoning
- B. XSS
- C. Iframe
- D. Session hijacking

Answer: B

Explanation:

QUESTION NO: 1564

A news and weather toolbar was accidentally installed into a web browser. The toolbar tracks users online activities and sends them to a central logging server. Which of the following attacks took place?

- A. Man-in-the-browser
- B. Flash cookies
- C. Session hijacking
- D. Remote code execution
- E. Malicious add-on

Answer: E

Explanation:

QUESTION NO: 1565

A project manager is working with an architectural firm that focuses on physical security. The project manager would like to provide requirements that support the primary goal of safety. Based on the project manager's desires, which of the following controls would the BEST to incorporate into the facility design?

- A. Biometrics
- B. Escape routers
- C. Reinforcements
- D. Access controls

Answer: B

Explanation:

QUESTION NO: 1566

While performing surveillance activities an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security controls?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

Answer: D

Explanation:

QUESTION NO: 1567

An administrator wants to configure a switch port so that it separates voice and data traffic. Which of the following **MUST** be configured on the switch port to enforce separation of traffic?

- A.** DMZ
- B.** VLAN
- C.** Subnetting
- D.** NAC

Answer: B

Explanation:

QUESTION NO: 1568

A company must send sensitive data over a non-secure network via web services. The company suspects that competitors are actively trying to intercept all transmissions. Some of the information may be valuable to competitors, even years after it has been sent. Which of the following will help mitigate the risk in the scenario?

- A.** Digitally sign the data before transmission
- B.** Choose stream ciphers over block ciphers
- C.** Use algorithms that allow for PFS
- D.** Enable TLS instead of SSL
- E.** Use a third party for key escrow

Answer: A

Explanation:

QUESTION NO: 1569

When implementing a mobile security strategy for an organization which of the following is the **MOST** influential concern that contributes to that organization's ability to extend enterprise policies to mobile devices?

- A. Support for mobile OS
- B. Support of mobile apps
- C. Availability of mobile browsers
- D. Key management for mobile devices

Answer: D

Explanation:

QUESTION NO: 1570

A recent review of accounts on various systems has found that after employees passwords are required to change they are recycling the same password as before. Which of the following policies should be enforced to prevent this from happening? (Select TWO)

- A. Reverse encryption
- B. Minimum password age
- C. Password complexity
- D. Account lockouts
- E. Password history
- F. Password expiration

Answer: B,E

Explanation:

QUESTION NO: 1571

A system administrator runs a network inventory scan every Friday at 10:00 am to track the progress of a large organization's operating system upgrade of all laptops. The system administrator discovers that some laptops are now only being reported as IP addresses. Which of the following options is MOST likely the cause of this issue?

- A. HIDS
- B. Host-based firewalls rules
- C. All the laptops are currently turned off
- D. DNS outage

Answer: B

Explanation:

QUESTION NO: 1572

A security administrator working for a law enforcement organization is asked to secure a computer system at the scene of a crime for transport to the law enforcement forensic facility. In order to capture as much evidence as possible, the computer system has been left running. The security administrator begins information by image which of the following system components FIRST?

- A. NVRAM
- B. RAM
- C. TPM
- D. SSD

Answer: B

Explanation:

QUESTION NO: 1573

A new employee has been hired to perform system administration duties across a large enterprise comprised of multiple separate security domains. Each remote location implements a separate security domain. The new employee has successfully responded to and fixed computer issues for the main office. When the new employee tries to perform work on remote computers, the following messages appears. You need permission to perform this action. Which of the following can be implemented to provide system administrators with the ability to perform administrative tasks on remote computers using their uniquely assigned account?

- A. Implement transitive trust across security domains
- B. Enable the trusted OS feature across all enterprise computers
- C. Install and configure the appropriate CA certificate on all domain controllers
- D. Verify that system administrators are in the domain administrator group in the main office

Answer: A

Explanation:

QUESTION NO: 1574

An administrator is hardening systems and wants to disable unnecessary services. One Linux server hosts files used by a Windows web server on another machine. The Linux server is only used for secure file transfer, but requires a share for the Windows web server as well. The administrator sees the following output from a netstat -1p command:

Proto	Recv-Q	Send-Q	Local Addr	Foreign Addr	State	PID
tcp	0	0	*:mysql	*:* LISTEN	1488/mysql	mysql
tcp	0	0	*:ftp	*:* LISTEN	2120/vsftpd	vsftpd
tcp	0	0	*:80	*:* LISTEN	1680/httpd	httpd
udp	0	0	*:69	*:* LISTEN	2680/tftp	tftp
tcp	0	0	*:139	*:* LISTEN	8217/smbd	smbd
tcp	0	0	*:6667	*:* LISTEN	2121/badBunny_FTP	badBunny_FTP

Which of the following processes can the administrator kill without risking impact to the purpose and function of the Linux or Windows servers? (Select Three)

- A. 1488
- B. 1680
- C. 2120
- D. 2121
- E. 2680
- F. 8217

Answer: A,D,F

Explanation:

QUESTION NO: 1575

A project manager is evaluating proposals for a cloud commuting project. The project manager is particularly concerned about logical security controls in place at the service provider's facility. Which of the following sections of the proposal would be MOST important to review, given the project manager's concerns?

- A. CCTV monitoring
- B. Perimeter security lighting system
- C. Biometric access system
- D. Environmental system configuration

Answer: C

Explanation:

QUESTION NO: 1576

A security administrator would like to ensure that some members of the building's maintenance staff are only allowed access to the facility during weekend hours. Access to the facility is

controlled by badge swipe and a man trap. Which of the following options will BEST accomplish this goal?

- A. CCTV
- B. Security Guard
- C. Time of day restrictions
- D. Job rotation

Answer: C

Explanation:

QUESTION NO: 1577

A security manager received reports of several laptops containing confidential data stolen out of a lab environment. The lab is not a high security area and is secured with physical key locks. The security manager has no information to provide investigators related to who may have stolen the laptops. Which of the following should the security manager implement to improve legal and criminal investigations in the future?

- A. Motion sensors
- B. Mobile device management
- C. CCTV
- D. Cable locks
- E. Full-disk encryption

Answer: C

Explanation:

QUESTION NO: 1578

During a Linux security audit at a local college, it was noted that members of the dean's group were able to modify employee records in addition to modifying student records, resulting in an audit exception. The college security policy states that the dean's group should only have the ability to modify student records. Assuming that the correct user and group ownerships are in place, which of the following sets of permissions should have been assigned to the directories containing the employee records?

- A. R-x---rwx
- B. Rwxrwxrwx
- C. Rwx----wx

D. Rwxrwxr—

Answer: B

Explanation:

QUESTION NO: 1579

An employee reports work was being completed on a company-owned laptop using a public wireless hot-spot. A pop-up screen appeared, and the user closed the pop-up. Seconds later, the desktop background was changed to the image of a padlock with a message demanding immediate payment to recover the data. Which of the following types of malware MOST likely caused this issue?

- A. Ransomware
- B. Rootkit
- C. Scareware
- D. Spyware

Answer: A

Explanation:

QUESTION NO: 1580

Which of the following can be mitigated with proper secure coding techniques?

- A. Input validation
- B. Error handling
- C. Header manipulation
- D. Cross-site scripting

Answer: A

Explanation:

QUESTION NO: 1581

Recently the desktop support group has been performing a hardware refresh and has replaced numerous computers. An auditor discovered that a number of the new computers did not have the company's antivirus software installed on them, Which of the following could be utilized to notify the network support group when computers without the antivirus software are added to the

network?

- A. Network port protection
- B. NAC
- C. NIDS
- D. Mac Filtering

Answer: C

Explanation:

QUESTION NO: 1582

An administrator needs to protect against downgrade attacks due to various vulnerabilities in SSL/TLS. Which of the following actions should be performed? (Select TWO)

- A. Set minimum protocol supported
- B. Request a new certificate from the CA
- C. Configure cipher order
- D. Disable flash cookie support
- E. Re-key the SSL certificate
- F. Add the old certificate to the CRL

Answer: C,E

Explanation:

QUESTION NO: 1583

A developer needs to utilize AES encryption in an application but requires the speed of encryption and decryption to be as fast as possible. The data that will be secured is not sensitive so speed is valued over encryption complexity. Which of the following would BEST satisfy these requirements?

- A. AES with output feedback
- B. AES with cipher feedback
- C. AES with cipher block chaining
- D. AES with counter mode

Answer: B

Explanation:

QUESTION NO: 1584

During a code review a software developer discovers a security risk that may result in hundreds of hours of rework. The security team has classified these issues as low risk. Executive management has decided that the code will not be rewritten. This is an example of:

- A. Risk avoidance
- B. Risk transference
- C. Risk mitigation
- D. Risk acceptance

Answer: D

Explanation:

QUESTION NO: 1585

A network was down for several hours due to a contractor entering the premises and plugging both ends of a network cable into adjacent network jacks. Which of the following would have prevented the network outage? (Select Two)

- A. Port security
- B. Loop Protection
- C. Implicit deny
- D. Log analysis
- E. Mac Filtering
- F. Flood Guards

Answer: A,F

Explanation:

QUESTION NO: 1586

After disabling SSID broadcast, a network administrator still sees the wireless network listed in available networks on a client laptop. Which of the following attacks may be occurring?

- A. Evil Twin
- B. ARP spoofing
- C. Disassociation flooding

- D. Rogue access point
- E. TKIP compromise

Answer: A

Explanation:

QUESTION NO: 1587

A security manager is preparing the training portion of an incident plan. Which of the following job roles should receive training on forensics, chain of custody, and the order of volatility?

- A. System owners
- B. Data custodians
- C. First responders
- D. Security guards

Answer: C

Explanation:

QUESTION NO: 1588

Virtualization that allows an operating system kernel to run multiple isolated instances of the guest is called:

- A. Process segregation
- B. Software defined network
- C. Containers
- D. Sandboxing

Answer: C

Explanation:

QUESTION NO: 1589

Which of the following is a proprietary protocol commonly used for router authentication across an enterprise?

- A. SAML

- B. TACACS
- C. LDAP
- D. RADIUS

Answer: B

Explanation:

QUESTION NO: 1590

While responding to an incident on a new Windows server, the administrator needs to disable unused services. Which of the following commands can be used to see processes that are listening on a TCP port?

- A. IPCONFIG
- B. Netstat
- C. PSINFO
- D. Net session

Answer: B

Explanation:

QUESTION NO: 1591

A system administrator must configure the company's authentication system to ensure that users will be unable to reuse the last ten passwords within a six months period. Which of the following settings must be configured? (Select Two)

- A. Minimum password age
- B. Password complexity
- C. Password history
- D. Minimum password length
- E. Multi-factor authentication
- F. Do not store passwords with reversible encryption

Answer: A,C

Explanation:

QUESTION NO: 1592

An administrator requests a new VLAN be created to support the installation of a new SAN. Which of the following data transport?

- A. Fibre Channel
- B. SAS
- C. Sonet
- D. ISCSI

Answer: A

Explanation:

QUESTION NO: 1593

Which of the following access control methodologies provides an individual with the most restrictive access rights to successfully perform their authorized duties?

- A. Mandatory Access Control
- B. Rule Based Access Control
- C. Least Privilege
- D. Implicit Deny
- E. Separation of Duties

Answer: C

Explanation:

QUESTION NO: 1594

An administrator wants to provide onboard hardware based cryptographic processing and secure key storage for full-disk encryption. Which of the following should the administrator use to fulfil the requirements?

- A. AES
- B. TPM
- C. FDE
- D. PAM

Answer: B

Explanation:

QUESTION NO: 1595

When viewing IPS logs the administrator see systems all over the world scanning the network for servers with port 22 open. The administrator concludes that this traffic is a(N):

- A. Risk
- B. Vulnerability
- C. Exploit
- D. Threat

Answer: D

Explanation:

QUESTION NO: 1596

Ann a user has been promoted from a sales position to sales manager. Which of the following risk mitigation strategies would be MOST appropriate when a user changes job roles?

- A. Implement data loss prevention
- B. Reset the user password
- C. User permissions review
- D. Notify incident management

Answer: C

Explanation:

QUESTION NO: 1597

A system administrator is implementing a firewall ACL to block specific communication to and from a predefined list of IP addresses, while allowing all other communication. Which of the following rules is necessary to support this implementation?

- A. Implicit allow as the last rule
- B. Implicit allow as the first rule
- C. Implicit deny as the first rule
- D. Implicit deny as the last rule

Answer: C

Explanation:

QUESTION NO: 1598

Joe a system architect wants to implement appropriate solutions to secure the company's distributed database. Which of the following concepts should be considered to help ensure data security? (Select TWO)

- A. Data at rest
- B. Data in use
- C. Replication
- D. Wiping
- E. Retention
- F. Cloud Storage

Answer: A,E

Explanation:

QUESTION NO: 1599

A forensics analyst is tasked identifying identical files on a hard drive. Due to the large number of files to be compared, the analyst must use an algorithm that is known to have the lowest collision rate. Which of the following should be selected?

- A. MD5
- B. RC4
- C. SHA-128
- D. AES-256

Answer: C

Explanation:

QUESTION NO: 1600

A government agency wants to ensure that the systems they use have been deployed as security as possible. Which of the following technologies will enforce protections on these systems to prevent files and services from operating outside of a strict rule set?

- A. Host based Intrusion detection
- B. Host-based firewall

- C. Trusted OS
- D. Antivirus

Answer: B

Explanation:

QUESTION NO: 1601

An organization receives an email that provides instruction on how to protect a system from being a target of new malware that is rapidly infecting systems. The incident response team investigates the notification and determines it to be invalid and notifies users to disregard the email. Which of the following best describes this occurrence?

- A. Phishing
- B. Scareware
- C. SPAM
- D. Hoax

Answer: D

Explanation:

QUESTION NO: 1602

Joe, an employee, has reported to Ann, a network technician, an unusual device plugged into a USB port on a workstation in the call center. Ann unplugs the workstation and brings it to the IT department where an incident is opened. Which of the following should have been done first?

- A. Notify the incident response team lead
- B. Document chain of custody
- C. Take a copy of volatile memory
- D. Make an image of the hard drive

Answer: A

Explanation:

QUESTION NO: 1603

A company is implementing a system to transfer direct deposit information to a financial institution. One of the requirements is that the financial institution must be certain that the deposit amounts

within the file have not been changed. Which of the following should be used to meet the requirement?

- A. Key escrow
- B. Perfect forward secrecy
- C. Transport encryption
- D. Digital signatures
- E. File encryption

Answer: D

Explanation:

QUESTION NO: 1604

An organization uses a Kerberos-based LDAP service for network authentication. The service is also utilized for internal web applications. Finally access to terminal applications is achieved using the same authentication method by joining the legacy system to the Kerberos realm. This company is using Kerberos to achieve which of the following?

- A. Trusted Operating System
- B. Rule-based access control
- C. Single sign on
- D. Mandatory access control

Answer: C

Explanation:

QUESTION NO: 1605

A recent audit has revealed that all employees in the bookkeeping department have access to confidential payroll information, while only two members of the bookkeeping department have job duties that require access to the confidential information. Which of the following can be implemented to reduce the risk of this information becoming compromised in this scenario? (Select TWO)

- A. Rule-based access control
- B. Role-based access control
- C. Data loss prevention
- D. Separation of duties
- E. Group-based permissions

Answer: B,E

Explanation:

QUESTION NO: 1606

A Chief Executive Officer (CEO) is steering company towards cloud computing. The CEO is requesting a federated sign-on method to have users sign into the sales application. Which of the following methods will be effective for this purpose?

- A. SAML
- B. RADIUS
- C. Kerberos
- D. LDAP

Answer: A

Explanation:

QUESTION NO: 1607

An administrator is configuring a new Linux web server where each user account is confined to a chroot jail. Which of the following describes this type of control?

- A. SysV
- B. Sandbox
- C. Zone
- D. Segmentation

Answer: B

Explanation:

QUESTION NO: 1608

Recently clients are stating they can no longer access a secure banking site's webpage. In reviewing the clients' web browser settings, the certificate chain is showing the following:

Certificate Chain:

X Digi Cert

Digi Cert High assurance C3

* banksite.com

Certificate Store:

Digi Cert – Others Certificate Store

Digi Cert High assurance C3 – Others Certificate Store

Based on the information provided, which of the following is the problem when connecting to the website?

- A. The certificate signature request was invalid
- B. Key escrow is failing for the certificate authority
- C. The certificate authority has revoked the certificate
- D. The clients do not trust the certificate authority

Answer: C

Explanation:

QUESTION NO: 1609

A company often processes sensitive data for the government. The company also processes a large amount of commercial work and as such is often providing tours to potential customers that take them into various workspaces. Which of the following security methods can provide protection against tour participants viewing sensitive information at minimal cost?

- A. Strong passwords
- B. Screen protectors
- C. Clean-desk policy
- D. Mantraps

Answer: C

Explanation:

QUESTION NO: 1610

Joe is a helpdesk specialist. During a routine audit, a company discovered that his credentials were used while he was on vacation. The investigation further confirmed that Joe still has his badge and it was last used to exit the facility. Which of the following access control methods is

MOST appropriate for preventing such occurrences in the future?

- A. Access control where the credentials cannot be used except when the associated badge is in the facility
- B. Access control where system administrators may limit which users can access their systems
- C. Access control where employee's access permissions is based on the job title
- D. Access control system where badges are only issued to cleared personnel

Answer: A

Explanation:

QUESTION NO: 1611

A security architect is designing an enterprise solution for the sales force of a corporation which handles sensitive customer data. The solution must allow users to work from remote offices and support traveling users. Which of the following is the MOST appropriate control for the architect to focus onto ensure confidentiality of data stored on laptops?

- A. Full-disk encryption
- B. Digital sign
- C. Federated identity management
- D. Cable locks

Answer: A

Explanation:

QUESTION NO: 1612

A security administrator needs a method to ensure that only employees can get onto the internal network when plugging into a network switch. Which of the following BEST meets that requirement?

- A. NAC
- B. UTM
- C. DMZ
- D. VPN

Answer: A

Explanation:

QUESTION NO: 1613

Having adequate lighting on the outside of a building is an example of which of the following security controls?

- A. Deterrent
- B. Compensating
- C. Detective
- D. Preventative

Answer: A

Explanation:

QUESTION NO: 1614

During a recent audit, it was discovered that several user accounts belonging to former employees were still active and had valid VPN permissions. Which of the following would help reduce the amount of risk the organization incurs in this situation in the future?

- A. Time-of-day restrictions
- B. User access reviews
- C. Group-based privileges
- D. Change management policies

Answer: B

Explanation:

QUESTION NO: 1615

An organization is working with a cloud services provider to transition critical business applications to a hybrid cloud environment. The organization retains sensitive customer data and wants to ensure the provider has sufficient administrative and logical controls in place to protect its data. In which of the following documents would this concern MOST likely be addressed?

- A. Service level agreement
- B. Interconnection security agreement
- C. Non-disclosure agreement
- D. Business process analysis

Answer: A

Explanation:

QUESTION NO: 1616

A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

- A. Mandatory access control
- B. Discretionary access control
- C. Role based access control
- D. Rule-based access control

Answer: C

Explanation:

QUESTION NO: 1617

Which of the following BEST describes an attack where communications between two parties are intercepted and forwarded to each party with neither party being aware of the interception and potential modification to the communications?

- A. Spear phishing
- B. Man-in-the-middle
- C. URL hijacking
- D. Transitive access

Answer: B

Explanation:

QUESTION NO: 1618

A security administrator wishes to implement a secure a method of file transfer when communicating with outside organizations. Which of the following protocols would BEST facilitate secure file transfers? (Select TWO)

- A. SCP

- B. TFTP
- C. SNMP
- D. FTP
- E. SMTP
- F. FTPS

Answer: A

Explanation:

QUESTION NO: 1619

A technician needs to implement a system which will properly authenticate users by their username and password only when the users are logging in from a computer in the office building. Any attempt to authenticate from a location other than the office building should be rejected. Which of the following **MUST** the technician implement?

- A. Dual factor authentication
- B. Transitive authentication
- C. Single factor authentication
- D. Biometric authentication

Answer: B

Explanation:

QUESTION NO: 1620

After correctly configuring a new wireless enabled thermostat to control the temperature of the company's meeting room, Joe, a network administrator determines that the thermostat is not connecting to the internet-based control system. Joe verifies that the thermostat received the expected network parameters and it is associated with the AP. Additionally, the other wireless mobile devices connected to the same wireless network are functioning properly. The network administrator verified that the thermostat works when tested at his residence. Which of the following is the **MOST** likely reason the thermostat is not connecting to the internet?

- A. The company implements a captive portal
- B. The thermostat is using the incorrect encryption algorithm
- C. the WPA2 shared key is incorrect
- D. The company's DHCP server scope is full

Answer: C

Explanation:

QUESTION NO: 1621

A Chief Security Officer (CSO) has been unsuccessful in attempts to access the website for a potential partner (www.example.net). Which of the following rules is preventing the CSO from accessing the site?

Blocked sites: *.nonews.com, *.rumorhasit.net, *.mars?

- A. Rule 1: deny from inside to outside source any destination any service smtp
- B. Rule 2: deny from inside to outside source any destination any service ping
- C. Rule 3: deny from inside to outside source any destination {blocked sites} service http-https
- D. Rule 4: deny from any to any source any destination any service any

Answer: C

Explanation:

QUESTION NO: 1622

Malware that changes its binary pattern on specific dates at specific times to avoid detection is known as a (n):

- A. armored virus
- B. logic bomb
- C. polymorphic virus
- D. Trojan

Answer: C

Explanation:

QUESTION NO: 1623

A company is planning to encrypt the files in several sensitive directories of a file server with a symmetric key. Which of the following could be used?

- A. RSA
- B. TwoFish
- C. Diffie-Helman

- D. NTLMv2
- E. RIPEMD

Answer: B

Explanation:

QUESTION NO: 1624

Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?

- A. MOU
- B. ISA
- C. BPA
- D. SLA

Answer: D

Explanation:

QUESTION NO: 1625

Which of the following are MOST susceptible to birthday attacks?

- A. Hashed passwords
- B. Digital certificates
- C. Encryption passwords
- D. One time passwords

Answer: A

Explanation:

QUESTION NO: 1626

Joe a computer forensic technician responds to an active compromise of a database server. Joe first collects information in memory, then collects network traffic and finally conducts an image of the hard drive. Which of the following procedures did Joe follow?

- A. Order of volatility

- B. Chain of custody
- C. Recovery procedure
- D. Incident isolation

Answer: A

Explanation:

QUESTION NO: 1627

A system administrator wants to implement an internal communication system that will allow employees to send encrypted messages to each other. The system must also support non-repudiation. Which of the following implements all these requirements?

- A. Bcrypt
- B. Blowfish
- C. PGP
- D. SHA

Answer: C

Explanation:

QUESTION NO: 1628

Given the log output:

```
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: msmith]  
[Source: 10.0.12.45]
```

```
[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
```

Which of the following should the network administrator do to protect data security?

- A. Configure port security for logons
- B. Disable telnet and enable SSH
- C. Configure an AAA server
- D. Disable password and enable RSA authentication

Answer: B

Explanation:

QUESTION NO: 1629

The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

- A. Certificate revocation list
- B. Intermediate authority
- C. Recovery agent
- D. Root of trust

Answer: B

Explanation:

QUESTION NO: 1630

The Chief Executive Officer (CEO) of a major defense contracting company is traveling overseas for a conference. The CEO will be taking a laptop. Which of the following should the security administrator implement to ensure confidentiality of the data if the laptop were to be stolen or lost during the trip?

- A. Remote wipe
- B. Full device encryption
- C. BIOS password
- D. GPS tracking

Answer: B

Explanation:

QUESTION NO: 1631

In an effort to reduce data storage requirements, a company decides to hash every file and eliminate duplicates. The data processing routines are time sensitive so the hashing algorithm is fast and supported on a wide range of systems. Which of the following algorithms is BEST suited for this purpose?

- A. MD5

- B. SHA
- C. RIPEMD
- D. AES

Answer: B

Explanation:

QUESTION NO: 1632

A new security policy in an organization requires that all file transfers within the organization be completed using applications that provide secure transfer. Currently, the organization uses FTP and HTTP to transfer files. Which of the following should the organization implement in order to be compliant with the new policy?

- A. Replace FTP with SFTP and replace HTTP with TLS
- B. Replace FTP with FTPS and replaces HTTP with TFTP
- C. Replace FTP with SFTP and replace HTTP with Telnet
- D. Replace FTP with FTPS and replaces HTTP with IPSec

Answer: B

Explanation:

QUESTION NO: 1633

A product manager is concerned about continuing operations at a facility located in a region undergoing significant political unrest. After consulting with senior management, a decision is made to suspend operations at the facility until the situation stabilizes. Which of the following risk management strategies BEST describes management's response?

- A. Deterrence
- B. Mitigation
- C. Avoidance
- D. Acceptance

Answer: C

Explanation:

QUESTION NO: 1634

Joe notices there are several user accounts on the local network generating spam with embedded malicious code. Which of the following technical control should Joe put in place to BEST reduce these incidents?

- A. Account lockout
- B. Group Based Privileges
- C. Least privilege
- D. Password complexity

Answer: A

Explanation:

QUESTION NO: 1635

Two users need to securely share encrypted files via email. Company policy prohibits users from sharing credentials or exchanging encryption keys. Which of the following can be implemented to enable users to share encrypted data while abiding by company policies?

- A. Key escrow
- B. Digital signatures
- C. PKI
- D. Hashing

Answer: B

Explanation:

QUESTION NO: 1636

An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient. Which of the following capabilities would be MOST appropriate to consider implementing in response to the new requirement?

- A. Transitive trust
- B. Symmetric encryption
- C. Two-factor authentication
- D. Digital signatures
- E. One-time passwords

Answer: D

Explanation:

QUESTION NO: 1637

Joe a website administrator believes he owns the intellectual property for a company invention and has been replacing image files on the company's public facing website in the DMZ. Joe is using steganography to hide stolen data. Which of the following controls can be implemented to mitigate this type of inside threat?

- A. Digital signatures
- B. File integrity monitoring
- C. Access controls
- D. Change management
- E. Stateful inspection firewall

Answer: B

Explanation:

QUESTION NO: 1638

The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?

- A. Collision resistance
- B. Rainbow table
- C. Key stretching
- D. Brute force attack

Answer: C

Explanation:

QUESTION NO: 1639

Which of the following is commonly used for federated identity management across multiple organizations?

- A. SAML

- B. Active Directory
- C. Kerberos
- D. LDAP

Answer: A

Explanation:

QUESTION NO: 1640

While performing surveillance activities, an attacker determines that an organization is using 802.1X to secure LAN access. Which of the following attack mechanisms can the attacker utilize to bypass the identified network security?

- A. MAC spoofing
- B. Pharming
- C. Xmas attack
- D. ARP poisoning

Answer: A

Explanation:

QUESTION NO: 1641

A security administrator has been asked to implement a VPN that will support remote access over IPSEC. Which of the following is an encryption algorithm that would meet this requirement?

- A. MD5
- B. AES
- C. UDP
- D. PKI

Answer: B

Explanation:

QUESTION NO: 1642

A security administrator is evaluating three different services: radius, diameter, and Kerberos. Which of the following is a feature that is UNIQUE to Kerberos?

- A. It provides authentication services
- B. It uses tickets to identify authenticated users
- C. It provides single sign-on capability
- D. It uses XML for cross-platform interoperability

Answer: B

Explanation:

QUESTION NO: 1643

Which of the following can affect electrostatic discharge in a network operations center?

- A. Fire suppression
- B. Environmental monitoring
- C. Proximity card access
- D. Humidity controls

Answer: D

Explanation:

QUESTION NO: 1644

a malicious attacker has intercepted HTTP traffic and inserted an ASCII line that sets the referrer URL. Which of the following is the attacker most likely utilizing?

- A. Header manipulation
- B. Cookie hijacking
- C. Cross-site scripting
- D. Xml injection

Answer: D

Explanation:

QUESTION NO: 1645

A company would like to prevent the use of a known set of applications from being used on company computers. Which of the following should the security administrator implement?

- A. Whitelisting
- B. Anti-malware
- C. Application hardening
- D. Blacklisting
- E. Disable removable media

Answer: D

Explanation:

QUESTION NO: 1646

A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

- A. Asset control
- B. Device access control
- C. Storage lock out
- D. Storage segmentation

Answer: B

Explanation:

QUESTION NO: 1647

A consultant has been tasked to assess a client's network. The client reports frequent network outages. Upon viewing the spanning tree configuration, the consultant notices that an old and low performing edge switch on the network has been elected to be the root bridge. Which of the following explains this scenario?

- A. The switch also serves as the DHCP server
- B. The switch has the lowest MAC address
- C. The switch has spanning tree loop protection enabled
- D. The switch has the fastest uplink port

Answer: C

Explanation:

QUESTION NO: 1648

An organization is trying to decide which type of access control is most appropriate for the network. The current access control approach is too complex and requires significant overhead. Management would like to simplify the access control and provide user with the ability to determine what permissions should be applied to files, document, and directories. The access control method that BEST satisfies these objectives is:

- A. Rule-based access control
- B. Role-based access control
- C. Mandatory access control
- D. Discretionary access control

Answer: B

Explanation:

QUESTION NO: 1649

While reviewing the security controls in place for a web-based application, a security controls assessor notices that there are no password strength requirements in place. Because of this vulnerability, passwords might be easily discovered using a brute force attack. Which of the following password requirements will MOST effectively improve the security posture of the application against these attacks? (Select two)

- A. Minimum complexity
- B. Maximum age limit
- C. Maximum length
- D. Minimum length
- E. Minimum age limit
- F. Minimum re-use limit

Answer: D,F

Explanation:

QUESTION NO: 1650

A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?

- A. Deploy antivirus software and configure it to detect and remove pirated software
- B. Configure the firewall to prevent the downloading of executable files
- C. Create an application whitelist and use OS controls to enforce it
- D. Prevent users from running as administrator so they cannot install software.

Answer: C

Explanation:

QUESTION NO: 1651

A security administrator is tasked with implementing centralized management of all network devices. Network administrators will be required to logon to network devices using their LDAP credentials. All command executed by network administrators on network devices must fall within a preset list of authorized commands and must be logged to a central facility. Which of the following configuration commands should be implemented to enforce this requirement?

- A. LDAP server 10.55.199.3
- B. CN=company, CN=com, OU=netadmin, DC=192.32.10.233
- C. SYSLOG SERVER 172.16.23.50
- D. TACAS server 192.168.1.100

Answer: B

Explanation:

QUESTION NO: 1652

A website administrator has received an alert from an application designed to check the integrity of the company's website. The alert indicated that the hash value for a particular MPEG file has changed. Upon further investigation, the media appears to be the same as it was before the alert. Which of the following methods has MOST likely been used?

- A. Cryptography
- B. Time of check/time of use
- C. Man in the middle
- D. Covert timing
- E. Steganography

Answer: E

Explanation:

QUESTION NO: 1653

An attacker captures the encrypted communication between two parties for a week, but is unable to decrypt the messages. The attacker then compromises the session key during one exchange and successfully compromises a single message. The attacker plans to use this key to decrypt previously captured and future communications, but is unable to. This is because the encryption scheme in use adheres to:

- A. Asymmetric encryption
- B. Out-of-band key exchange
- C. Perfect forward secrecy
- D. Secure key escrow

Answer: A

Explanation:

QUESTION NO: 1654

Many employees are receiving email messages similar to the one shown below:

From IT department

To employee

Subject email quota exceeded

Please click on the following link <http://www.website.info/email.php?quota=1Gb> and provide your username and password to increase your email quota. Upon reviewing other similar emails, the security administrator realized that all the phishing URLs have the following common elements; they all use HTTP, they all come from .info domains, and they all contain the same URI.

Which of the following should the security administrator configure on the corporate content filter to prevent users from accessing the phishing URL, while at the same time minimizing false positives?

- A. BLOCK http://www.*.info/
- B. DROP <http://www.website.info/email.php?>
- C. Redirect http://www.*.info/email.php?quota=*TOhttp://company.com/corporate_policy.html
- D. DENY http://*.info/email.php?quota=1Gb

Answer: D

Explanation:

QUESTION NO: 1655

A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:

```
10:55:24.126586 IP 192.168.1.10.5000 > 172.31.67.4.21: Flags[S]  
10:55:24.126596 IP 192.168.1.10.5001 > 172.31.67.4.22: Flags[S]  
10:55:24.126601 IP 192.168.1.10.5002 > 172.31.67.4.25: Flags[S]  
10:55:24.126608 IP 192.168.1.10.5003 > 172.31.67.4.37: Flags[S]
```

Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?

- A. DENY TCO From ANY to 172.31.64.4
- B. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
- C. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
- D. Deny TCP from 192.168.1.10 to 172.31.67.4

Answer: D

Explanation:

QUESTION NO: 1656

The IT department needs to prevent users from installing untested applications. Which of the following would provide the BEST solution?

- A. Job rotation
- B. Least privilege
- C. Account lockout
- D. Antivirus

Answer: B

Explanation:

QUESTION NO: 1657

An attack that is using interference as its main attack to impede network traffic is which of the following?

- A. Introducing too much data to a targets memory allocation
- B. Utilizing a previously unknown security flaw against the target
- C. Using a similar wireless configuration of a nearby network
- D. Inundating a target system with SYN requests

Answer: A

Explanation:

QUESTION NO: 1658

An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys. Which of the following algorithms is appropriate for securing the key exchange?

- A. DES
- B. Blowfish
- C. DSA
- D. Diffie-Hellman
- E. 3DES

Answer: D

Explanation:

QUESTION NO: 1659

Ann, a college professor, was recently reprimanded for posting disparaging remarks re-grading her coworkers on a web site. Ann stated that she was not aware that the public was able to view her remakes. Which of the following security-related trainings could have made Ann aware of the repercussions of her actions?

- A. Data Labeling and disposal
- B. Use of social networking
- C. Use of P2P networking
- D. Role-based training

Answer: B

Explanation:

QUESTION NO: 1660

During a recent audit, it was discovered that many services and desktops were missing security patches. Which of the following BEST describes the assessment that was performed to discover this issue?

- A. Network mapping
- B. Vulnerability scan
- C. Port Scan
- D. Protocol analysis

Answer: B

Explanation:

QUESTION NO: 1661

When generating a request for a new x.509 certificate for securing a website, which of the following is the MOST appropriate hashing algorithm?

- A. RC4
- B. MD5
- C. HMAC
- D. SHA

Answer: B

Explanation:

QUESTION NO: 1662

The administrator installs database software to encrypt each field as it is written to disk. Which of the following describes the encrypted data?

- A. In-transit
- B. In-use
- C. Embedded
- D. At-rest

Answer: B

Explanation:

QUESTION NO: 1663

Which of the following allows an application to securely authenticate a user by receiving credentials from a web domain?

- A. TACACS+
- B. RADIUS
- C. Kerberos
- D. SAML

Answer: D

Explanation:

QUESTION NO: 1664

A network technician is trying to determine the source of an ongoing network based attack. Which of the following should the technician use to view IPv4 packet data on a particular internal network segment?

- A. Proxy
- B. Protocol analyzer
- C. Switch
- D. Firewall

Answer: B

Explanation:

QUESTION NO: 1665

The security administrator has noticed cars parking just outside of the building fence line. Which of the following security measures can the administrator use to help protect the company's WiFi network against war driving? (Select TWO)

- A. Create a honeynet
- B. Reduce beacon rate

- C. Add false SSIDs
- D. Change antenna placement
- E. Adjust power level controls
- F. Implement a warning banner

Answer: A,E

Explanation:

QUESTION NO: 1666

A security administrator suspects that data on a server has been exfiltrated as a result of unauthorized remote access. Which of the following would assist the administrator in confirming the suspicions? (Select TWO)

- A. Networking access control
- B. DLP alerts
- C. Log analysis
- D. File integrity monitoring
- E. Host firewall rules

Answer: B,C

Explanation:

QUESTION NO: 1667

A company is deploying a new VoIP phone system. They require 99.999% uptime for their phone service and are concerned about their existing data network interfering with the VoIP phone system. The core switches in the existing data network are almost fully saturated. Which of the following options will provide the best performance and availability for both the VoIP traffic, as well as the traffic on the existing data network?

- A. Put the VoIP network into a different VLAN than the existing data network.
- B. Upgrade the edge switches from 10/100/1000 to improve network speed
- C. Physically separate the VoIP phones from the data network
- D. Implement flood guards on the data network

Answer: A

Explanation:

QUESTION NO: 1668

A server administrator needs to administer a server remotely using RDP, but the specified port is closed on the outbound firewall on the network. The access the server using RDP on a port other than the typical registered port for the RDP protocol?

- A. TLS
- B. MPLS
- C. SCP
- D. SSH

Answer: A

Explanation:

QUESTION NO: 1669

Which of the following can be used to control specific commands that can be executed on a network infrastructure device?

- A. LDAP
- B. Kerberos
- C. SAML
- D. TACACS+

Answer: D

Explanation:

QUESTION NO: 1670

Company XYZ has decided to make use of a cloud-based service that requires mutual, certificate-based authentication with its users. The company uses SSL-inspecting IDS at its network boundary and is concerned about the confidentiality of the mutual authentication. Which of the following model prevents the IDS from capturing credentials used to authenticate users to the new service or keys to decrypt that communication?

- A. Use of OATH between the user and the service and attestation from the company domain
- B. Use of active directory federation between the company and the cloud-based service
- C. Use of smartcards that store x.509 keys, signed by a global CA
- D. Use of a third-party, SAML-based authentication service for attestation

Answer: B

Explanation:

QUESTION NO: 1671

Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it. Which of the following BEST describes what the company?

- A. The system integration phase of the SDLC
- B. The system analysis phase of SSDSLC
- C. The system design phase of the SDLC
- D. The system development phase of the SDLC

Answer: B

Explanation:

QUESTION NO: 1672

A company is investigating a data compromise where data exfiltration occurred. Prior to the investigation, the supervisor terminates an employee as a result of the suspected data loss. During the investigation, the supervisor is absent for the interview, and little evidence can be provided from the role-based authentication system in use by the company. The situation can be identified for future mitigation as which of the following?

- A. Job rotation
- B. Log failure
- C. Lack of training
- D. Insider threat

Answer: B

Explanation:

QUESTION NO: 1673

A security administrator needs an external vendor to correct an urgent issue with an organization's

physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?

- A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
- B. Have the external vendor come onsite and provide access to the PACS directly
- C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
- D. Set up a web conference on the administrator's pc; then remotely connect to the pacs

Answer: C

Explanation:

QUESTION NO: 1674

A datacenter manager has been asked to prioritize critical system recovery priorities. Which of the following is the MOST critical for immediate recovery?

- A. Communications software
- B. Operating system software
- C. Weekly summary reports to management
- D. Financial and production software

Answer: B

Explanation:

QUESTION NO: 1675

Which of the following techniques can be bypass a user or computer's web browser privacy settings? (Select Two)

- A. SQL injection
- B. Session hijacking
- C. Cross-site scripting
- D. Locally shared objects
- E. LDAP injection

Answer: B,C

Explanation:

QUESTION NO: 1676

When designing a web based client server application with single application server and database cluster backend, input validation should be performed:

- A. On the client
- B. Using database stored procedures
- C. On the application server
- D. Using HTTPS

Answer: C

Explanation:

QUESTION NO: 1677

Which of the following delineates why it is important to perform egress filtering and monitoring on Internet connected security zones of interfaces on a firewall?

- A. Egress traffic is more important than ingress traffic for malware prevention
- B. To rebalance the amount of outbound traffic and inbound traffic
- C. Outbound traffic could be communicating to known botnet sources
- D. To prevent DDoS attacks originating from external network

Answer: B

Explanation:

QUESTION NO: 1678

The help desk is receiving numerous password change alerts from users in the accounting department. These alerts occur multiple times on the same day for each of the affected users' accounts. Which of the following controls should be implemented to curtail this activity?

- A. Password Reuse
- B. Password complexity
- C. Password History
- D. Password Minimum age

Answer: D

Explanation:

QUESTION NO: 1679

Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)

- A. Block level encryption
- B. SAML authentication
- C. Transport encryption
- D. Multifactor authentication
- E. Predefined challenge questions
- F. Hashing

Answer: B,D

Explanation:

QUESTION NO: 1680

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

```
VPN log:
[2015-03-25 08:00.23 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.29 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:00.40 CST-6: VPN-Server-1: User1 5.5.5.5 authentication failed. Wrong password.]
[2015-03-25 08:01.11 CST-6: VPN-Server-1: User1 5.5.5.5 authentication succeeded.]
[2015-03-25 09:01.35 CST-6: VPN-Server-1: User1 5.5.5.5 disconnected. Idle timeout.]
Corporate firewall log:
[2015-03-25 14:01.12 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.13 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.14 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.15 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.16 CST: accepted 5.5.5.5(1025) -> 10.1.1.5(3389)]
[2015-03-25 14:01.17 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
[2015-03-25 14:01.18 CST: denied 5.5.5.5(icmp) -> 10.1.1.5(icmp)]
Workstation host firewall log:
[2015-03-21 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-22 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-23 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-24 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
[2015-03-25 09:01.17 CST-5: 5.5.5.5 -> 10.1.1.5(msrdp) (action=drop)]
[2015-03-26 08:00.00 CST-5: 10.1.1.5 -> www.hackersite11111.com(https) (action=allow)]
```

Which of the following is preventing the remote user from being able to access the workstation?

- A. Network latency is causing remote desktop service request to time out
- B. User1 has been locked out due to too many failed passwords
- C. Lack of network time synchronization is causing authentication mismatches
- D. The workstation has been compromised and is accessing known malware sites
- E. The workstation host firewall is not allowing remote desktop connections

Answer: B

Explanation:

QUESTION NO: 1681

During a data breach cleanup, it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem best be revisited?

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons learned

Answer: A

Explanation:

QUESTION NO: 1682

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most likely recommend during the audit out brief?

- A. Discretionary access control for the firewall team
- B. Separation of duties policy for the firewall team
- C. Least privilege for the firewall team
- D. Mandatory access control for the firewall team

Answer: B

Explanation:

QUESTION NO: 1683

Which of the following is the appropriate network structure used to protect servers and services that must be provided to external clients without completely eliminating access for internal users?

- A. NAC
- B. VLAN

- C. DMZ
- D. Subnet

Answer: C

Explanation:

QUESTION NO: 1684

An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the server. Which of the following will most likely fix the uploading issue for the users?

- A. Create an ACL to allow the FTP service write access to user directories
- B. Set the Boolean selinux value to allow FTP home directory uploads
- C. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
- D. Configure the FTP daemon to utilize PAM authentication pass through user permissions

Answer: A

Explanation:

QUESTION NO: 1685

An administrator thinks the UNIX systems may be compromised, but a review of system log files provides no useful information. After discussing the situation with the security team, the administrator suspects that the attacker may be altering the log files and removing evidence of intrusion activity. Which of the following actions will help detect attacker attempts to further alter log files?

- A. Enable verbose system logging
- B. Change the permissions on the user's home directory
- C. Implement remote syslog
- D. Set the bash_history log file to "read only"

Answer: C

Explanation:

QUESTION NO: 1686

A global gaming console manufacturer is launching a new gaming platform to its customers. Which of the following controls reduces the risk created by malicious gaming customers attempting to circumvent control by way of modifying consoles?

- A. Firmware version control
- B. Manual software upgrades
- C. Vulnerability scanning
- D. Automatic updates
- E. Network segmentation
- F. Application firewalls

Answer: A,D

Explanation:

QUESTION NO: 1687

An audit has revealed that database administrators are also responsible for auditing database changes and backup logs. Which of the following access control methodologies would BEST mitigate this concern?

- A. Time of day restrictions
- B. Principle of least privilege
- C. Role-based access control
- D. Separation of duties

Answer: D

Explanation:

QUESTION NO: 1688

Ann, a security administrator, has been instructed to perform fuzz-based testing on the company's applications. Which of the following best describes what she will do?

- A. Enter random or invalid data into the application in an attempt to cause it to fault
- B. Work with the developers to eliminate horizontal privilege escalation opportunities
- C. Test the applications for the existence of built-in- back doors left by the developers
- D. Hash the application to verify it won't cause a false positive on the HIPS.

Answer: A

Explanation:**QUESTION NO: 1689**

Joe, a technician, is working remotely with his company provided laptop at the coffee shop near his home. Joe is concerned that another patron of the coffee shop may be trying to access his laptop. Which of the following is an appropriate control to use to prevent the other patron from accessing Joe's laptop directly?

- A. full-disk encryption
- B. Host-based firewall
- C. Current antivirus definitions
- D. Latest OS updates

Answer: B

Explanation:

QUESTION NO: 1690

An attacker uses a network sniffer to capture the packets of a transaction that adds \$20 to a gift card. The attacker then user a function of the sniffer to push those packets back onto the network again, adding another \$20 to the gift card. This can be done many times. Which of the following describes this type of attack?

- A. Integer overflow attack
- B. Smurf attack
- C. Replay attack
- D. Buffer overflow attack
- E. Cross-site scripting attack

Answer: C

Explanation:

QUESTION NO: 1691

An organization is moving its human resources system to a cloud services provider. The company plans to continue using internal usernames and passwords with the service provider, but the security manager does not want the service provider to have a company of the passwords. Which

of the following options meets all of these requirements?

- A. Two-factor authentication
- B. Account and password synchronization
- C. Smartcards with PINS
- D. Federated authentication

Answer: D

Explanation:

QUESTION NO: 1692

The data backup window has expanded into the morning hours and has begun to affect production users. The main bottleneck in the process is the time it takes to replicate the backups to separate servers at the offsite data center. Which of the following uses of deduplication could be implemented to reduce the backup window?

- A. Implement deduplication at the network level between the two locations
- B. Implement deduplication on the storage array to reduce the amount of drive space needed
- C. Implement deduplication on the server storage to reduce the data backed up
- D. Implement deduplication on both the local and remote servers

Answer: B

Explanation:

QUESTION NO: 1693

A penetration testing is preparing for a client engagement in which the tester must provide data that proves and validates the scanning tools' results. Which of the following is the best method for collecting this information?

- A. Set up the scanning system's firewall to permit and log all outbound connections
- B. Use a protocol analyzer to log all pertinent network traffic
- C. Configure network flow data logging on all scanning system
- D. Enable debug level logging on the scanning system and all scanning tools used.

Answer: A

Explanation:

QUESTION NO: 1694

Which of the following best describes the initial processing phase used in mobile device forensics?

- A.** The phone should be powered down and the battery removed to preserve the state of data on any internal or removable storage utilized by the mobile device
- B.** The removable data storage cards should be processed first to prevent data alteration when examining the mobile device
- C.** The mobile device should be examined first, then removable storage and lastly the phone without removable storage should be examined again
- D.** The phone and storage cards should be examined as a complete unit after examining the removable storage cards separately.

Answer: A

Explanation:

QUESTION NO: 1695

Ann a security analyst is monitoring the IDS console and noticed multiple connections from an internal host to a suspicious call back domain \. Which of the following tools would aid her to decipher the network traffic?

- A.** Vulnerability Scanner
- B.** NMAP
- C.** NETSTAT
- D.** Packet Analyzer

Answer: C

Explanation:

QUESTION NO: 1696

An administrator is testing the collision resistance of different hashing algorithms. Which of the following is the strongest collision resistance test?

- A.** Find two identical messages with different hashes
- B.** Find two identical messages with the same hash
- C.** Find a common has between two specific messages
- D.** Find a common hash between a specific message and a random message

Answer: A

Explanation:**QUESTION NO: 1697**

The SSID broadcast for a wireless router has been disabled but a network administrator notices that unauthorized users are accessing the wireless network. The administrator has determined that attackers are still able to detect the presence of the wireless network despite the fact the SSID has been disabled. Which of the following would further obscure the presence of the wireless network?

- A. Upgrade the encryption to WPA or WPA2
- B. Create a non-zero length SSID for the wireless router
- C. Reroute wireless users to a honeypot
- D. Disable responses to a broadcast probe request

Answer: D

Explanation:**QUESTION NO: 1698**

Which of the following should be used to implement voice encryption?

- A. SSLv3
- B. VDSL
- C. SRTP
- D. VoIP

Answer: C

Explanation:**QUESTION NO: 1699**

During an application design, the development team specifies a LDAP module for single sign-on communication with the company's access control database. This is an example of which of the following?

- A. Application control
- B. Data in-transit
- C. Identification

D. Authentication

Answer: D

Explanation:

QUESTION NO: 1700

After a merger, it was determined that several individuals could perform the tasks of a network administrator in the merged organization. Which of the following should have been performed to ensure that employees have proper access?

- A. Time-of-day restrictions**
- B. Change management**
- C. Periodic auditing of user credentials**
- D. User rights and permission review**

Answer: D

Explanation:

QUESTION NO: 1701

A company exchanges information with a business partner. An annual audit of the business partner is conducted against the SLA in order to verify:

- A. Performance and service delivery metrics**
- B. Backups are being performed and tested**
- C. Data ownership is being maintained and audited**
- D. Risk awareness is being adhered to and enforced**

Answer: A

Explanation:

QUESTION NO: 1702

Which of the following is the proper way to quantify the total monetary damage resulting from an exploited vulnerability?

- A. Calculate the ALE**

- B. Calculate the ARO
- C. Calculate the MTBF
- D. Calculate the TCO

Answer: A

Explanation:

QUESTION NO: 1703

A security administrator needs to implement a system that detects possible intrusions based upon a vendor provided list. Which of the following BEST describes this type of IDS?

- A. Signature based
- B. Heuristic
- C. Anomaly-based
- D. Behavior-based

Answer: A

Explanation:

QUESTION NO: 1704

The chief Security Officer (CSO) has reported a rise in data loss but no break ins have occurred. By doing which of the following is the CSO most likely to reduce the number of incidents?

- A. Implement protected distribution
- B. Empty additional firewalls
- C. Conduct security awareness training
- D. Install perimeter barricades

Answer: A

Explanation:

QUESTION NO: 1705

During a data breach cleanup it is discovered that not all of the sites involved have the necessary data wiping tools. The necessary tools are quickly distributed to the required technicians, but when should this problem BEST be revisited?

- A. Reporting
- B. Preparation
- C. Mitigation
- D. Lessons Learned

Answer: B

Explanation:

QUESTION NO: 1706

New magnetic locks were ordered for an entire building. In accordance with company policy, employee safety is the top priority. In case of a fire where electricity is cut, which of the following should be taken into consideration when installing the new locks?

- A. Fail safe
- B. Fault tolerance
- C. Fail secure
- D. Redundancy

Answer: A

Explanation:

QUESTION NO: 1707

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

- A. It can protect multiple domains
- B. It provides extended site validation
- C. It does not require a trusted certificate authority
- D. It protects unlimited subdomains

Answer: B

Explanation:

QUESTION NO: 1708

After a merger between two companies a security analyst has been asked to ensure that the

organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

- A. Monitor VPN client access
- B. Reduce failed login out settings
- C. Develop and implement updated access control policies
- D. Review and address invalid login attempts
- E. Increase password complexity requirements
- F. Assess and eliminate inactive accounts

Answer: E,F

Explanation:

QUESTION NO: 1709

A new mobile application is being developed in-house. Security reviews did not pick up any major flaws, however vulnerability scanning results show fundamental issues at the very end of the project cycle. Which of the following security activities should also have been performed to discover vulnerabilities earlier in the lifecycle?

- A. Architecture review
- B. Risk assessment
- C. Protocol analysis
- D. Code review

Answer: D

Explanation:

QUESTION NO: 1710

A security administrator is creating a subnet on one of the corporate firewall interfaces to use as a DMZ which is expected to accommodate at most 14 physical hosts. Which of the following subnets would BEST meet the requirements?

- A. 192.168.0.16 255.255.255.248
- B. 192.168.0.16/28
- C. 192.168.1.50 255.255.255.240
- D. 192.168.2.32/27

Answer: B

Explanation:

QUESTION NO: 1711

A company has a security policy that specifies all endpoint computing devices should be assigned a unique identifier that can be tracked via an inventory management system. Recent changes to airline security regulations have caused many executives in the company to travel with mini tablet devices instead of laptops. These tablet devices are difficult to tag and track. An RDP application is used from the tablet to connect into the company network. Which of the following should be implemented in order to meet the security policy requirements?

- A. Virtual desktop infrastructure (VDI)
- B. WS-security and geo-fencing
- C. A hardware security module (HSM)
- D. RFID tagging system
- E. MDM software
- F. Security Requirements Traceability Matrix (SRTM)

Answer: E

Explanation:

QUESTION NO: 1712

The security administrator receives an email on a non-company account from a coworker stating that some reports are not exporting correctly. Attached to the email was an example report file with several customers' names and credit card numbers with the PIN. Which of the following is the BEST technical controls that will help mitigate this risk of disclosing sensitive data?

- A. Configure the mail server to require TLS connections for every email to ensure all transport data is encrypted
- B. Create a user training program to identify the correct use of email and perform regular audits to ensure compliance
- C. Implement a DLP solution on the email gateway to scan email and remove sensitive data or files
- D. Classify all data according to its sensitivity and inform the users of data that is prohibited to share

Answer: C

Explanation:

QUESTION NO: 1713

A technician is configuring a wireless guest network. After applying the most recent changes the technician finds the new devices can no longer find the wireless network by name but existing devices are still able to use the wireless network. Which of the following security measures did the technician MOST likely implement to cause this Scenario?

- A. Deactivation of SSID broadcast
- B. Reduction of WAP signal output power
- C. Activation of 802.1X with RADIUS
- D. Implementation of MAC filtering
- E. Beacon interval was decreased

Answer: A

Explanation:

QUESTION NO: 1714

A security administrator has been assigned to review the security posture of the standard corporate system image for virtual machines. The security administrator conducts a thorough review of the system logs, installation procedures, and network configuration of the VM image. Upon reviewing the access logs and user accounts, the security administrator determines that several accounts will not be used in production. Which of the following would correct the deficiencies?

- A. Mandatory access controls
- B. Disable remote login
- C. Host hardening
- D. Disabling services

Answer: C

Explanation:

QUESTION NO: 1715

Although a web enabled application appears to only allow letters in the comment field of a web form, malicious user was able to carry a SQL injection attack by sending special characters through the web comment field. Which of the following has the application programmer failed to

implement?

- A. Revision control system
- B. Client side exception handling
- C. Server side validation
- D. Server hardening

Answer: C

Explanation:

QUESTION NO: 1716

An attacker discovers a new vulnerability in an enterprise application. The attacker takes advantage of the vulnerability by developing new malware. After installing the malware the attacker is provided with access to the infected machine. Which of the following is being described?

- A. Zero-day exploit
- B. Remote code execution
- C. Session hijacking
- D. Command injection

Answer: A

Explanation:

QUESTION NO: 1717

A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine. Which of the following can be implemented to reduce the likelihood of this attack going undetected?

- A. Password complexity rules
- B. Continuous monitoring
- C. User access reviews
- D. Account lockout policies

Answer: B

Explanation:

QUESTION NO: 1718

A bank requires tellers to get manager approval when a customer wants to open a new account. A recent audit shows that there have been four cases in the previous year where tellers opened accounts without management approval. The bank president thought separation of duties would prevent this from happening. In order to implement a true separation of duties approach the bank could:

- A. Require the use of two different passwords held by two different individuals to open an account
- B. Administer account creation on a role based access control approach
- C. Require all new accounts to be handled by someone else other than a teller since they have different duties
- D. Administer account creation on a rule based access control approach

Answer: C

Explanation:

QUESTION NO: 1719

A security administrator has been tasked with improving the overall security posture related to desktop machines on the network. An auditor has recently that several machines with confidential customer information displayed in the screens are left unattended during the course of the day. Which of the following could the security administrator implement to reduce the risk associated with the finding?

- A. Implement a clean desk policy
- B. Security training to prevent shoulder surfing
- C. Enable group policy based screensaver timeouts
- D. Install privacy screens on monitors

Answer: C

Explanation:

QUESTION NO: 1720

Company policy requires the use of passphrases instead of passwords. Which of the following technical controls **MUST** be in place in order to promote the use of passphrases?

- A. Reuse
- B. Length
- C. History
- D. Complexity

Answer: D

Explanation:

QUESTION NO: 1721

During a routine audit, it is discovered that someone has been using a stale administrator account to log into a seldom used server. The person has been using the server to view inappropriate websites that are prohibited to end users. Which of the following could best prevent this from occurring again?

- A. Credential management
- B. Group policy management
- C. Acceptable use policy
- D. Account expiration policy

Answer: B

Explanation:

QUESTION NO: 1722

Which of the following should identify critical systems and components?

- A. MOU
- B. BPA
- C. ITCP
- D. BCP

Answer: D

Explanation:

QUESTION NO: 1723

Which of the following works by implanting software on systems but delays execution until a specific set of conditions is met?

- A. Logic bomb
- B. Trojan
- C. Scareware
- D. Ransomware

Answer: A

Explanation:

QUESTION NO: 1724

A web application is configured to target browsers and allow access to bank accounts to siphon money to a foreign account. This is an example of which of the following attacks?

- A. SQL injection
- B. Header manipulation
- C. Cross-site scripting
- D. Flash cookie exploitation

Answer: C

Explanation:

QUESTION NO: 1725

Technicians working with servers hosted at the company's datacenter are increasingly complaining of electric shocks when touching metal items which have been linked to hard drive failures. Which of the following should be implemented to correct this issue?

- A. Decrease the room temperature
- B. Increase humidity in the room
- C. Utilize better hot/cold aisle configurations
- D. Implement EMI shielding

Answer: D

Explanation:

QUESTION NO: 1726

A portable data storage device has been determined to have malicious firmware. Which of the following is the BEST course of action to ensure data confidentiality?

- A. Format the device
- B. Re-image the device
- C. Perform virus scan in the device
- D. Physically destroy the device

Answer: C

Explanation:

QUESTION NO: 1727

A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable. Which of the following MUST be implemented to support this requirement?

- A. CSR
- B. OCSP
- C. CRL
- D. SSH

Answer: C

Explanation:

QUESTION NO: 1728

A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?

- A. Gray box vulnerability testing
- B. Passive scan
- C. Credentialed scan
- D. Bypassing security controls

Answer: A

Explanation:

QUESTION NO: 1729

The Chief Security Officer (CISO) at a multinational banking corporation is reviewing a plan to upgrade the entire corporate IT infrastructure. The architecture consists of a centralized cloud environment hosting the majority of data, small server clusters at each corporate location to handle the majority of customer transaction processing, ATMs, and a new mobile banking application accessible from smartphones, tablets, and the Internet via HTTP. The corporation does business having varying data retention and privacy laws. Which of the following technical modifications to the architecture and corresponding security controls should be implemented to provide the MOST complete protection of data?

- A.** Revoke exiting root certificates, re-issue new customer certificates, and ensure all transactions are digitally signed to minimize fraud, implement encryption for data in-transit between data centers
- B.** Ensure all data is encryption according to the most stringent regulatory guidance applicable, implement encryption for data in-transit between data centers, increase data availability by replicating all data, transaction data, logs between each corporate location
- C.** Store customer data based on national borders, ensure end-to end encryption between ATMs, end users, and servers, test redundancy and COOP plans to ensure data is not inadvertently shifted from one legal jurisdiction to another with more stringent regulations
- D.** Install redundant servers to handle corporate customer processing, encrypt all customer data to ease the transfer from one country to another, implement end-to-end encryption between mobile applications and the cloud.

Answer: C

Explanation:

QUESTION NO: 1730

While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy. Which of the following tool or technology would work BEST for obtaining more information on this traffic?

- A.** Firewall logs
- B.** IDS logs
- C.** Increased spam filtering
- D.** Protocol analyzer

Answer: B

Explanation:

QUESTION NO: 1731

A network administrator wants to ensure that users do not connect any unauthorized devices to the company network. Each desk needs to connect a VoIP phone and computer. Which of the following is the BEST way to accomplish this?

- A. Enforce authentication for network devices
- B. Configure the phones on one VLAN, and computers on another
- C. Enable and configure port channels
- D. Make users sign an Acceptable use Agreement

Answer: A

Explanation:

QUESTION NO: 1732

An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?

- A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
- B. Configure the smart phones so that the stored data can be destroyed from a centralized location
- C. Configure the smart phones so that all data is saved to removable media and kept separate from the device
- D. Enable GPS tracking on all smart phones so that they can be quickly located and recovered

Answer: A

Explanation:

QUESTION NO: 1733

A user of the wireless network is unable to gain access to the network. The symptoms are:

- 1.) Unable to connect to both internal and Internet resources

2.) The wireless icon shows connectivity but has no network access

The wireless network is WPA2 Enterprise and users must be a member of the wireless security group to authenticate. Which of the following is the MOST likely cause of the connectivity issues?

- A. The wireless signal is not strong enough
- B. A remote DDoS attack against the RADIUS server is taking place
- C. The user's laptop only supports WPA and WEP
- D. The DHCP scope is full
- E. The dynamic encryption key did not update while the user was offline

Answer: A

Explanation:

QUESTION NO: 1734

A chief Financial Officer (CFO) has asked the Chief Information Officer (CISO) to provide responses to a recent audit report detailing deficiencies in the organization security controls. The CFO would like to know ways in which the organization can improve its authorization controls. Given the request by the CFO, which of the following controls should the CISO focus on in the report? (Select Three)

- A. Password complexity policies
- B. Hardware tokens
- C. Biometric systems
- D. Role-based permissions
- E. One time passwords
- F. Separation of duties
- G. Multifactor authentication
- H. Single sign-on
- I. Least privilege

Answer: D,F,I

Explanation:

QUESTION NO: 1735

A mobile device user is concerned about geographic positioning information being included in messages sent between users on a popular social network platform. The user turns off the functionality in the application, but wants to ensure the application cannot re-enable the setting

without the knowledge of the user. Which of the following mobile device capabilities should the user disable to achieve the stated goal?

- A. Device access control
- B. Location based services
- C. Application control
- D. GEO-Tagging

Answer: D

Explanation:

QUESTION NO: 1736

A member of a digital forensics team, Joe arrives at a crime scene and is preparing to collect system data. Before powering the system off, Joe knows that he must collect the most volatile data first. Which of the following is the correct order in which Joe should collect the data?

- A. CPU cache, paging/swap files, RAM, remote logging data
- B. RAM, CPU cache, Remote logging data, paging/swap files
- C. Paging/swap files, CPU cache, RAM, remote logging data
- D. CPU cache, RAM, paging/swap files, remote logging data

Answer: B

Explanation:

QUESTION NO: 1737

An organization has hired a penetration tester to test the security of its ten web servers. The penetration tester is able to gain root/administrative access in several servers by exploiting vulnerabilities associated with the implementation of SMTP, POP, DNS, FTP, Telnet, and IMAP. Which of the following recommendations should the penetration tester provide to the organization to better protect their web servers in the future?

- A. Use a honeypot
- B. Disable unnecessary services
- C. Implement transport layer security
- D. Increase application event logging

Answer: B

Explanation:

QUESTION NO: 1738

A security engineer is faced with competing requirements from the networking group and database administrators. The database administrators would like ten application servers on the same subnet for ease of administration, whereas the networking group would like to segment all applications from one another. Which of the following should the security administrator do to rectify this issue?

- A.** Recommend performing a security assessment on each application, and only segment the applications with the most vulnerability
- B.** Recommend classifying each application into like security groups and segmenting the groups from one another
- C.** Recommend segmenting each application, as it is the most secure approach
- D.** Recommend that only applications with minimal security features should be segmented to protect them

Answer: B

Explanation:

QUESTION NO: 1739

A security analyst has been asked to perform a review of an organization's software development lifecycle. The analyst reports that the lifecycle does not contain a phase in which team members evaluate and provide critical feedback of another developer's code. Which of the following assessment techniques is BEST described in the analyst's report?

- A.** Architecture evaluation
- B.** Baseline reporting
- C.** Whitebox testing
- D.** Peer review

Answer: D

Explanation:

QUESTION NO: 1740

An attacker wearing a building maintenance uniform approached a company's receptionist asking for access to a secure area. The receptionist asks for identification, a building access badge and checks the company's list approved maintenance personnel prior to granting physical access to

the secure are. The controls used by the receptionist are in place to prevent which of the following types of attacks?

- A. Tailgating
- B. Shoulder surfing
- C. Impersonation
- D. Hoax

Answer: C

Explanation:

QUESTION NO: 1741

A security administrator is tasked with conducting an assessment made to establish the baseline security posture of the corporate IT infrastructure. The assessment must report actual flaws and weaknesses in the infrastructure. Due to the expense of hiring outside consultants, the testing must be performed using in-house or cheaply available resource. There cannot be a possibility of any requirement being damaged in the test. Which of the following has the administrator been tasked to perform?

- A. Risk transference
- B. Penetration test
- C. Threat assessment
- D. Vulnerability assessment

Answer: D

Explanation:

QUESTION NO: 1742

A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website. During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine. Which of the following describes the type of attack the proxy has been legitimately programmed to perform?

- A. Transitive access
- B. Spoofing
- C. Man-in-the-middle
- D. Replay

Answer: C

Explanation:

QUESTION NO: 1743

Which of the following use the SSH protocol?

- A. Stelnet
- B. SCP
- C. SNMP
- D. FTPS
- E. SSL
- F. SFTP

Answer: B,F

Explanation:

QUESTION NO: 1744

A security administrator is developing training for corporate users on basic security principles for personal email accounts. Which of the following should be mentioned as the MOST secure way for password recovery?

- A. Utilizing a single question for password recovery
- B. Sending a PIN to a smartphone through text message
- C. Utilizing CAPTCHA to avoid brute force attacks
- D. Use a different e-mail address to recover password

Answer: B

Explanation:

QUESTION NO: 1745

A company researched the root cause of a recent vulnerability in its software. It was determined that the vulnerability was the result of two updates made in the last release. Each update alone would not have resulted in the vulnerability. In order to prevent similar situations in the future, the company should improve which of the following?

- A. Change management procedures
- B. Job rotation policies
- C. Incident response management
- D. Least privilege access controls

Answer: A

Explanation:

QUESTION NO: 1746

A computer on a company network was infected with a zero-day exploit after an employee accidentally opened an email that contained malicious content. The employee recognized the email as malicious and was attempting to delete it, but accidentally opened it. Which of the following should be done to prevent this scenario from occurring again in the future?

- A. Install host-based firewalls on all computers that have an email client installed
- B. Set the email program default to open messages in plain text
- C. Install end-point protection on all computers that access web email
- D. Create new email spam filters to delete all messages from that sender

Answer: C

Explanation:

QUESTION NO: 1747

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage. Which of the following should be implemented?

- A. Recovery agent
- B. Ocsf
- C. Crl
- D. Key escrow

Answer: B

Explanation:

QUESTION NO: 1748

An administrator intends to configure an IPSec solution that provides ESP with integrity protection, but not confidentiality protection. Which of the following AES modes of operation would meet this integrity-only requirement?

- A. GMAC
- B. PCBC
- C. CBC
- D. GCM
- E. CFB

Answer: A

Explanation:

QUESTION NO: 1749

The chief security officer (CSO) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs. Which of the following is the best solution for the network administrator to secure each internal website?

- A. Use certificates signed by the company CA
- B. Use a signing certificate as a wild card certificate
- C. Use certificates signed by a public ca
- D. Use a self-signed certificate on each internal server

Answer: A

Explanation:

QUESTION NO: 1750

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base. Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

- A. Peer review
- B. Component testing
- C. Penetration testing
- D. Vulnerability testing

Answer: D

